



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED

AUG 21 2001

Technology Center 2100

Re the Application of

Takahiro SUGIMOTO

Application No.: 09/853,708

Filed: May 14, 2001

Docket No.: 109460

For: METHOD AND APPARATUS FOR ESTABLISHING A SECURITY POLICY, AND
METHOD AND APPARATUS FOR SUPPORTING ESTABLISHMENT OF SECURITY
POLICY

CLAIM FOR PRIORITY

Director of the U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

The benefit of the filing dates of the following prior foreign applications filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. § 119 is hereby claimed:

Japanese Patent Application No. 2000-164819 filed June 1, 2000; and

Japanese Patent Application No. 2001-132177 filed April 27, 2001.

In support of this claim, certified copies of said original foreign applications:

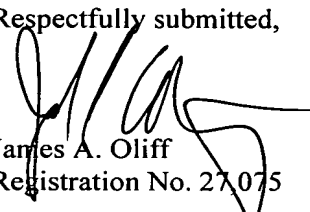
 X are filed herewith.

 were filed on in Parent Application No. filed .

 will be filed at a later date.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. § 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of these documents.

Respectfully submitted,


James A. Oliff
Registration No. 27,075

Joel S. Armstrong
Registration No. 36,430

JAO:JSA/zmc
Date: August 17, 2001

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE
AUTHORIZATION

Please grant any extension
necessary for entry;

Charge any fee due to our
Deposit Account No. 15-0461



日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2001年 4月27日

出願番号

Application Number:

特願2001-132177

出願人

Applicant(s):

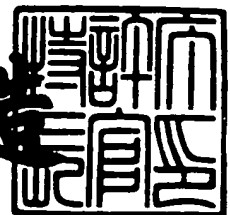
株式会社アズジェント

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月18日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3041847

【書類名】 特許願

【整理番号】 ASG-0002

【提出日】 平成13年 4月27日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 5/00

【発明者】

【住所又は居所】 東京都中央区日本橋小網町 1 9 番 7 号 株式会社アズジェント内

【氏名】 杉本 ▲隆▼洋

【特許出願人】

【識別番号】 500056448

【氏名又は名称】 株式会社アズジェント

【代理人】

【識別番号】 100109014

【弁理士】

【氏名又は名称】 伊藤 充

【電話番号】 03-5366-2677

【先の出願に基づく優先権主張】

【出願番号】 特願2000-164819

【出願日】 平成12年 6月 1日

【手数料の表示】

【予納台帳番号】 067081

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0008652

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティポリシー構築方法及び装置並びにセキュリティポリシー構築を支援する方法及び装置

【特許請求の範囲】

【請求項 1】 所定の団体のセキュリティポリシーを構築する方法において

セキュリティポリシーのドラフトを構築するドラフト構築ステップと、
前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップと、

前記差異に基づき前記セキュリティポリシーのドラフトの調整、又は、前記差異に基づき前記団体の実際の情報システムの運用ルールの調整、を行う調整ステップと、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項 2】 請求項 1 記載のセキュリティポリシー構築方法において、

前記ドラフト構築ステップは、

団体に属するメンバーにするべき質問を生成する生成ステップと、

生成した前記質問を前記メンバーに聞く質問ステップと、

前記質問に対する前記メンバーの回答を取得する回答取得ステップと、

前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築ステップと、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項 3】 請求項 2 記載のセキュリティポリシー構築方法において、

前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項 4】 請求項 2 記載のセキュリティポリシー構築方法において、

前記回答取得ステップは、

前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行

し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すステップと、

の少なくとも1のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項5】 請求項2記載のセキュリティポリシー構築方法において、前記分析ステップは、

前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、

前記回答群によって仮想的に想定される情報システムと、前記セキュリティポリシーと、の比較をし差異を検査する第1差異検出ステップと、

前記回答群によって仮想的に想定される情報システムを実際の情報システムの調査でプルーフし、このプルーフした情報システムと、前記セキュリティポリシーのドラフトと、を比較をし差異を検査する第2差異検出ステップと、

の少なくとも1のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項6】 請求項5記載のセキュリティポリシー構築方法において、前記調査した差異の対策をその優先度と共に立てる対策ステップ、を含むことを特徴とするセキュリティポリシー構築方法。

【請求項7】 請求項1記載のセキュリティポリシー構築方法において、前記団体のセキュリティ状況を診断する診断ステップ、を含み、この診断ステップの診断結果を前記団体に提示することによって、前記団体がセキュリティポリシーの必要性を認識しうることを特徴とするセキュリティポリシー構築方法。

【請求項8】 請求項6記載のセキュリティポリシー構築方法において、前記優先度と共に立てたセキュリティ対策の実行を、その優先度に合わせて計画し、団体の予算化を実現するプライオリティプランニングステップ、を含むことを特徴とするセキュリティポリシー構築方法。

【請求項 9】 請求項 8 記載のセキュリティポリシー構築方法において、
前記セキュリティ対策には、
セキュリティポリシー作成を管理する体制を作ることと、
セキュリティシステムの導入と、
セキュリティポリシーを遵守するための従業員の教育と、
システムログの分析と、
ネットワーク監視と、
セキュリティポリシーに基づく運用の監査と、
セキュリティポリシーの見直しと、
が含まれることを特徴とするセキュリティポリシー構築方法。

【請求項 10】 請求項 8 記載のセキュリティポリシー構築方法において、
前記計画に合わせて、前記セキュリティ対策を実行するセキュリティ強化策実行ステップ、
を含むことを特徴とするセキュリティポリシー構築方法。

【請求項 11】 セキュリティポリシーを構築する方法において、
団体に属するメンバーにすべき質問を生成する生成ステップと、
生成した前記質問を前記メンバーに聞く質問ステップと、
前記質問に対する前記メンバーの回答を取得する回答取得ステップと、
前記取得した回答に基づき、セキュリティポリシーを構築する構築ステップと
を含むことを特徴とするセキュリティポリシー構築方法。

【請求項 12】 請求項 11 記載のセキュリティポリシー構築方法において
前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成すること
を特徴とするセキュリティポリシー構築方法。

【請求項 13】 請求項 11 記載のセキュリティポリシー構築方法において
前記回答取得ステップは、
前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問

者の回答として前記記憶手段中に保管するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すステップと、

の少なくとも1のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項14】 請求項11記載のセキュリティポリシー構築方法において

前記構築ステップは、

グローバルガイドラインに準拠して、前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、

前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、

前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、

の3レベルのセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項15】 請求項14記載のセキュリティポリシー構築方法において

前記コーポレートレベルポリシーは、

前記団体全体の情報セキュリティシステムの基準を記述し、前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述することを特徴とするセキュリティポリシー構築方法。

【請求項16】 請求項14記載のセキュリティポリシー構築方法において

前記プロダクトレベルポリシーは、

自然言語で情報セキュリティシステムを構成する各構成装置の設定を記述する

第1レベルと、

特定商品の特定言語で情報セキュリティシステムを構成する各構成装置の設定を記述する第2レベルと、

の2種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築方法。

【請求項17】 請求項11記載のセキュリティポリシー構築方法において

前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップ、

を含み、

前記分析ステップは、

前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、

前記回答群によって仮想的に想定される情報システムと、前記セキュリティポリシーと、の比較をし差異を検査する第1差異検出ステップと、

前記回答群によって仮想的に想定される情報システムを実際の情報システムの調査でプルーフし、このプルーフした情報システムと、前記セキュリティポリシーのドラフトと、を比較をし差異を検査する第2差異検出ステップと、

の少なくとも1個のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項18】 請求項17記載のセキュリティポリシー構築方法において

前記調査した差異の対策をその優先度と共に立てる対策ステップ、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項19】 セキュリティポリシーを構築するセキュリティポリシー構築装置において、

団体に属するメンバーにするべき質問を生成する質問生成手段と、

前記生成した質問に対する回答を保管する記憶手段と、

前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手

段と、

前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、

を含むことを特徴とするセキュリティポリシー構築装置。

【請求項 2 0】 請求項 1 9 記載のセキュリティポリシー構築装置において

前記質問生成手段は、被質問者の職務内容に基づき、前記被質問者にすべき質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項 2 1】 請求項 1 9 記載のセキュリティポリシー構築装置において

前記回答保管手段は、

前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、

又は、

前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納し、

又は、

前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示す、

ことを特徴とするセキュリティポリシー構築装置。

【請求項 2 2】 請求項 1 9 記載のセキュリティポリシー構築装置において

前記構築手段は、

前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、

前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、

前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシ

一の基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、
の3レベルのセキュリティポリシーを構築することを特徴とするセキュリティ
ポリシー構築装置。

【請求項23】 請求項22記載のセキュリティポリシー構築装置において

、
前記コーポレートレベルポリシーは、

前記団体全体の情報セキュリティシステムの基準を記述し、前記団体の情報セ
キュリティシステムを構成する各ユニットの個々の基準を記述することを特徴と
するセキュリティポリシー構築装置。

【請求項24】 請求項22記載のセキュリティポリシー構築装置において

、
前記プロダクトレベルポリシーは、

自然言語で情報セキュリティシステムを構成する各構成装置の設定を記述する
第1レベルと、

特定商品の特定言語で情報セキュリティシステムを構成する各構成装置の設定
を記述する第2レベルと、

の2種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポ
リシー構築装置。

【請求項25】 団体のセキュリティ状況を評価する評価方法において、

前記団体に属するメンバーにするべき質問を生成する質問生成ステップと、

前記生成した質問を前記メンバーに聞く質問ステップと、

前記質問に対する前記メンバーの回答を取得する回答取得ステップと、

前記取得した回答に基づき、セキュリティ状況を評価するセキュリティ状況評
価ステップと、

を含むことを特徴とする評価方法。

【請求項26】 請求項25記載の評価方法において、

前記質問生成ステップは、被質問者の職務内容に基づき、前記被質問者にする
べき質問を生成することを特徴とする評価方法。

【請求項27】 請求項25記載の評価方法において、

前記回答保管ステップは、

前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として記憶手段中に保管することを特徴とする評価方法。

【請求項 2 8】 請求項 2 5 記載の評価方法において、

前記セキュリティ状況の評価は、

前記団体のセキュリティの評価と、

前記団体が属する産業分野に含まれる他の団体のセキュリティの評価の平均と

前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの評価の最高値と、

を含むことを特徴とする評価方法。

【請求項 2 9】 請求項 2 5 記載の評価方法において、

前記セキュリティ状況の評価は、

セキュリティに対する理解と姿勢、

前記団体のセキュリティ体制、

不測事態対応、

セキュリティに関する予算化、

セキュリティ改善措置、

の各項目に関する点数を含むことを特徴とする評価方法。

【請求項 3 0】 団体のセキュリティの状況进行评估する評価装置において、

団体に属するメンバーにするべき質問を出力する出力手段と、

前記生成した質問に対する回答を保管する記憶手段と、

前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、

前記保管した回答に基づき、団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手段と、

を含むことを特徴とする評価装置。

【請求項 3 1】 請求項 3 0 記載の評価装置において、

前記回答保管手段は、

前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として前記記憶手段中に保管することを特徴とする評価装置。

【請求項 3 2】 請求項 3 0 記載の評価装置において、

前記セキュリティ完成度報告書は、

前記団体のセキュリティの完成度と、

前記団体が属する産業分野に含まれる他の団体のセキュリティの完成度の平均と、

前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの完成度の最高値と、

を含むことを特徴とする評価装置。

【請求項 3 3】 請求項 3 0 記載の評価装置において、

前記セキュリティ完成度報告書は、

セキュリティに対する理解と姿勢、

団体のセキュリティ体制、

不測事態対応、

セキュリティに関する予算化、

セキュリティ改善措置、

の各項目に関する点数を含むことを特徴とする評価装置。

【請求項 3 4】 セキュリティポリシーと、団体の情報システムとの差異を分析する分析装置において、

団体のメンバーに質問をすることによって得られた回答群に含まれる個々の回答の間に矛盾があるか否か検査する矛盾検査手段と、

前記検査した矛盾に関する情報を出力する矛盾出力手段と、

を含むことを特徴とする分析装置。

【請求項 3 5】 請求項 3 4 記載の分析装置において、

前記矛盾に関する情報に基づき、前記回答群中の矛盾点を指摘する指摘手段と

前記指摘手段が指摘した矛盾点が解決された回答群に基づき、団体の情報システムの構成を仮想的に構築する構築手段と、

前記仮想的に構築した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、
を含むことを特徴とする分析装置。

【請求項 3 6】 請求項 3 5 記載の分析装置において、

前記団体の情報システムを調査し、前記情報システムの構成を入力する実システム入力手段と、

前記情報システムの構成によって、前記仮想的に構成した情報システムをブルーフシ、ブルーフ後の前記仮想的に構成した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、
を含むことを特徴とする分析装置。

【請求項 3 7】 請求項 2 記載のセキュリティポリシー構築方法において、

前記生成ステップは、前記団体の業種に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項 3 8】 請求項 1 1 記載のセキュリティポリシー構築方法において

前記生成ステップは、前記団体の業種に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項 3 9】 請求項 1 9 記載のセキュリティポリシー構築装置において

前記質問生成手段は、前記団体の業種に基づき、被質問者にすべき質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項 4 0】 請求項 2 記載のセキュリティポリシー構築方法において、

前記構築ステップは、

特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項 4 1】 請求項 1 1 記載のセキュリティポリシー構築方法において

前記構築ステップは、

特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項 4 2】 請求項 1 9 記載のセキュリティポリシー構築装置において

前記構築手段は、特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項 4 3】 請求項 2 記載のセキュリティポリシー構築方法において、

前記構築ステップは、利用者が指示した 1 種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項 4 4】 請求項 4 3 記載のセキュリティポリシー構築方法において

前記生成ステップは、利用者が指示した 1 種類又は複数種類のグローバルガイドラインに基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項 4 5】 請求項 1 1 記載のセキュリティポリシー構築方法において

前記構築ステップは、利用者が指示した 1 種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項 4 6】 請求項 4 5 記載のセキュリティポリシー構築方法において

前記生成ステップは、利用者が指示した 1 種類又は複数種類のグローバルガイドラインに基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項 4 7】 請求項 1 9 記載のセキュリティポリシー構築装置において

前記構築手段は、利用者が指示した1種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項48】 請求項47記載のセキュリティポリシー構築装置において

前記質問生成手段は、利用者が指示した1種類又は複数種類のグローバルガイドラインに基づき、被質問者にすべき質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項49】 請求項2記載のセキュリティポリシー構築方法において、前記構築ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項50】 請求項49記載のセキュリティポリシー構築方法において

前記生成ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項51】 請求項11記載のセキュリティポリシー構築方法において

前記構築ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項52】 請求項51記載のセキュリティポリシー構築方法において

前記生成ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項53】 請求項19記載のセキュリティポリシー構築装置において

前記構築手段は、利用者が指示したセキュリティポリシーの強度指標に基づき

、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項 5 4】 請求項 5 0 記載のセキュリティポリシー構築装置において

前記質問生成手段は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項 5 5】 セキュリティポリシーの強度を調整するセキュリティポリシー強度調整方法において、

前記セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整ステップと、

前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力ステップと、

を含むことを特徴とするセキュリティポリシー強度調整方法。

【請求項 5 6】 セキュリティポリシーの強度を調整するセキュリティポリシー強度調整装置において、

前記セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手段と、

前記強度指標に合致していたルールと、前記強度調整手段が置き換えたルールとを、合成して出力する合成出力手段と、

を含むことを特徴とするセキュリティポリシー強度調整装置。

【請求項 5 7】 所定の団体のセキュリティポリシーを構築する方法において、

前記団体のセキュリティポリシーを構築するために必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する生成ステップと、

生成した前記質問をメンバーに聞く質問ステップと、

前記質問に対する前記メンバーの回答を取得する取得ステップと、

前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築

ステップと、

を含み、

前記構築ステップは、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項58】 請求項57記載のセキュリティポリシー構築方法において

前記生成ステップは、利用者が指示した構築範囲に関する質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項59】 所定の団体のセキュリティポリシーを構築するセキュリティポリシー構築装置において、

前記団体のセキュリティポリシーを構築するために必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する質問生成手段と、

前記生成した質問に対する回答を保管する記憶手段と、

前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、

前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、

を含み、

前記構築手段は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項60】 請求項59記載のセキュリティポリシー構築装置において

前記質問生成手段は、利用者が指示した構築範囲に関する質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項61】 所定の団体のセキュリティポリシーを構築するのに必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する質問生成手順と、

前記生成した質問に対する回答を入力し、記憶手段に格納する回答保管手順と

前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 6 2】 請求項 6 1 記載の記録媒体において、

前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にすべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 6 3】 請求項 6 1 記載の記録媒体において、

前記回答保管手順は、

前記入力した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、

又は、

前記入力した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、最終的な回答を推定し、推定した回答を示すことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 6 4】 請求項 6 1 記載の記録媒体において、

前記質問生成手順は、前記団体の業種に基づき、前記被質問者にすべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 6 5】 請求項 6 1 記載の記録媒体において、

前記構築手順は、利用者が指示した 1 種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 6 6】 請求項 6 1 記載の記録媒体において、

前記質問生成手順は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項 6 7】 請求項 6 1 記載の記録媒体において、

前記構築手順は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項68】 所定の団体のセキュリティの完成度を評価するために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問を出力する質問出力手順と、

前記出力した質問に対する回答を入力し、記憶手段に格納する回答保管手順と、

前記記憶手段に保管した前記回答に基づき、前記団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項69】 請求項68記載の記録媒体において、

前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にすべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項70】 所定の団体のセキュリティポリシーと、前記団体の情報システムとの差異を知るために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問に対する回答群中の個々の回答間に矛盾があるか否かを検査する矛盾検査手順と、

前記検査した矛盾に関する情報を出力する矛盾出力手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項71】 請求項70記載の記録媒体において、

前記矛盾に関する情報に基づき、前記回答群中の矛盾点を指摘する矛盾点指摘手順と、

前記指摘された矛盾点を解決した回答群に基づき、前記団体の情報システムの構成を仮想的に構築する構築手順と、

前記仮想的に構築した情報システムの構成と、前記セキュリティポリシーとを比較し、両者の差異を出力する差異出力手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項72】 セキュリティポリシー中の個々のルールであって、利用者

が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手順と、

前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 7 3】 所定の団体のセキュリティポリシーを構築するのに必要な事項に関する質問であって、前記団体に属するメンバーにすべき質問を生成する質問生成手順と、

前記生成した質問に対する回答を入力し、記憶手段に保管する回答保管手順と

前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手順と、

をコンピュータに実行させるためのプログラム。

【請求項 7 4】 請求項 7 3 記載のプログラムにおいて、

前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にすべき質問を生成することを特徴とするプログラム。

【請求項 7 5】 請求項 7 3 記載のプログラムにおいて、

前記回答保管手順は、

前記入力した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、

又は、

前記入力した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すことを特徴とするプログラム。

【請求項 7 6】 請求項 7 3 記載のプログラムにおいて、

前記質問生成手順は、前記団体の業種に基づき、前記被質問者にすべき質問を生成することを特徴とするプログラム。

【請求項 7 7】 請求項 7 3 記載のプログラムにおいて、

前記構築手順は、利用者が指示した 1 種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするプログラム。

【請求項 7 8】 請求項 7 3 記載のプログラムにおいて、

前記質問生成手順は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするプログラム。

【請求項 7 9】 請求項 7 3 記載のプログラムにおいて、

前記構築手順は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするプログラム。

【請求項 8 0】 所定の団体のセキュリティの完成度を評価するために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問を出力する質問出力手順と、

前記出力した質問に対する回答を入力し、記憶手段に保管する回答保管手順と

前記記憶手段に保管した前記回答に基づき、前記団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手順と、
をコンピュータに実行させるためのプログラム。

【請求項 8 1】 所定の団体のセキュリティポリシーと、前記団体の情報システムとの差異を知るために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問に対する回答群中の個々の回答間に矛盾があるか否かを検査する矛盾検査手順と、

前記検査した矛盾に関する情報を出力する矛盾出力手順と、

をコンピュータに実行させるためのプログラム。

【請求項 8 2】 請求項 8 1 記載のプログラムにおいて、

前記矛盾に関する情報に基づき、前記回答群の整合をとり、矛盾点を解決した回答群を生成する整合手順と、

前記整合した後の回答群に基づき、前記団体の情報システムの構成を仮想的に構築する構築手順と、

前記仮想的に構築した情報システムの構成と、前記セキュリティポリシーとを

比較し、両者の差異を出力する差異出力手順と、

をコンピュータに実行させるためのプログラム。

【請求項 8 3】 セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手順と、

前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力手順と、

をコンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、いわゆるセキュリティポリシーの構築に関する。特に、各団体に適合したセキュリティポリシーを迅速に構築可能な方法・装置、及びセキュリティポリシーの構築を支援する方法・装置に関する。

【 0 0 0 2 】

【従来の技術】

情報技術の発達と共に、情報セキュリティの重要性が増している。団体においては、団体内部の情報を保護するために種々の手段が講じられている。

【 0 0 0 3 】

たとえば、外部のネットワークと接続する部分にはいわゆるファイアーウォールを設け、他者が無断で内部のネットワークに侵入したり、内部の情報にアクセスしてしまうことを防止している。

【 0 0 0 4 】

また、コンピュータウィルス等を駆逐するために、ウィルス検出・駆除ソフトウェアに団体内部のコンピュータを監視させている。なお、本文においては、「団体」とは、企業その他、国や地方公共団体の機関、財団法人等各種法人、その他の団体・組織を意味する。

【 0 0 0 5 】

さて、上述したように、従来から種々の手段が情報セキュリティの確保のため

に用いられている。

【0006】

しかしながら、各手段を別個独立に議論・検討していたのでは、団体全体としてのセキュリティ強度を確保することは困難である。

【0007】

たとえば、いくらファイアーウォールを強化しても、団体の建物内に自由に第三者が入ってくることができ、そこにある端末を操作できるのであれば、団体全体としてのセキュリティ強度は著しく低下してしまう。

【0008】

さらに、ウィルス検出ソフトウェアを用いていても、新たなウィルスに対抗可能とするためにソフトウェアの更新を怠っていれば、新しいコンピュータウィルスには対抗できない。

【0009】

したがって、団体全体としても情報セキュリティの強度を高くするためには、団体全体としての、情報セキュリティに対する設計及び実現手法を作りあげることが必要である。この設計及び実現手法（群）を一般にセキュリティポリシーと呼ぶ。

【0010】

【発明が解決しようとする課題】

このセキュリティポリシーは、もちろん各団体毎に異なる項目、内容を有するものであるが、標準的なセキュリティポリシーを構築するための基本的な項目、内容が、国際的なガイドラインとして種々提案されている。

【0011】

このような汎用的なガイドラインは存在するが、現実には有用なセキュリティポリシーは、個々の団体毎に構築する必要がある。したがって、大量生産できるものではないため、セキュリティポリシーの構築には多大な労力と時間が必要であった。

【0012】

さらに、セキュリティポリシーは、時間経過と共にその内容を変更する必要が

ある。たとえば、社内の組織が変更された場合には、それに応じて既存情報の利用価値やリスク評価の変更が生じ、それに見合ったセキュリティポリシーを変更しなければならない。

【 0 0 1 3 】

従来は、セキュリティポリシーの構築・定期的な修正等に関する一般的な手法は知られておらず、個々のシステムエンジニアが経験と勘に頼って、セキュリティポリシーの構築・修正を行っている。その結果、セキュリティポリシーの構築・修正に多大な労力が必要となってしまう、ともすれば、修正が団体と実状の変化に追いつけない事態も想定される。

【 0 0 1 4 】

したがって、セキュリティポリシーと団体の実状がかけ離れてしまい、強固な情報セキュリティを構築・維持することが困難な場合も見受けられた。

【 0 0 1 5 】

本発明は、係る課題に鑑みなされたものであり、その目的は、セキュリティポリシーを効率的に構築する方法及びセキュリティポリシーの構築を支援する装置を提供することである。

【 0 0 1 6 】

【課題を解決するための手段】

本発明は、上記課題を解決するために、所定の団体のセキュリティポリシーを構築する方法において、セキュリティポリシーのドラフトを構築するドラフト構築ステップと、前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップと、前記差異に基づき前記セキュリティポリシーのドラフトの調整、又は、前記差異に基づき前記団体の実際の情報システムの運用ルールの調整、を行う調整ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【 0 0 1 7 】

このような構成によって、セキュリティポリシーの構築を段階的に行うことができ、効率的なセキュリティポリシーの構築を行うことができる。

【 0 0 1 8 】

また、本発明は、前記ドラフト構築ステップは、団体に属するメンバーにするべき質問を生成する生成ステップと、生成した前記質問を前記メンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する回答取得ステップと、前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【0019】

このような構成によって、質問に基づきセキュリティポリシーのドラフトを構築できる。

【0020】

また、本発明は、前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【0021】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【0022】

また、本発明は、前記回答取得ステップは、前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すステップと、の少なくとも1のステップを含むことを特徴とするセキュリティポリシー構築方法である。

【0023】

このような構成によって、複数人で分散して質問をした場合に、得られた回答を統合することが可能である。

【0024】

また、本発明は、前記分析ステップは、前記取得した回答群中に矛盾する回答

が含まれているか否かを検査する矛盾検査ステップと、前記回答群によって仮想的に想定される情報システムと、前記セキュリティポリシーと、の比較をし差異を検査する第1差異検出ステップと、前記回答群によって仮想的に想定される情報システムを実際の情報システムの調査でプルーフし、このプルーフした情報システムと、前記セキュリティポリシーのドラフトと、を比較をし差異を検査する第2差異検出ステップと、の少なくとも1のステップを含むことを特徴とするセキュリティポリシー構築方法である。

【0025】

このような構成によって、回答間の矛盾を知ることができ、さらに、実システムとセキュリティポリシーの差異を検出することが可能である。

【0026】

また、本発明は、前記調査した差異の対策をその優先度と共に立てる対策ステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【0027】

このような構成によって、優先度を含めた対策を講じることが可能である。

【0028】

また、本発明は、前記団体のセキュリティ状況を診断する診断ステップ、を含み、この診断ステップの診断結果を前記団体に提示することによって、前記団体がセキュリティポリシーの必要性を認識しうることを特徴とするセキュリティポリシー構築方法である。

【0029】

このような構成によって、団体のセキュリティ状況を知ることができる。

【0030】

また、本発明は、前記優先度と共に立てたセキュリティ対策の実行を、その優先度に合わせて計画し、団体の予算化を実現するプライオリティプランニングステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【0031】

このような構成によって、セキュリティ対策を計画的に実行することができ、予算を立てることが容易となる。

【0032】

また、本発明は、前記セキュリティ対策には、セキュリティポリシー作成を管理する体制を作ることと、セキュリティシステムの導入と、セキュリティポリシーを遵守するための従業員の教育と、システムログの分析と、ネットワーク監視と、セキュリティポリシーに基づく運用の監査と、セキュリティポリシーの見直しと、が含まれることを特徴とするセキュリティポリシー構築方法である。

【0033】

情報セキュリティ機器の導入だけでなく、従業員の教育等も含まれるので、高い情報セキュリティを達成することができる。

【0034】

また、本発明は、前記計画に合わせて、前記セキュリティ対策を実行するセキュリティ強化策実行ステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【0035】

このような構成によって、セキュリティ対策を円滑に実行に移すことが可能である。

【0036】

また、本発明は、セキュリティポリシーを構築する方法において、団体に属するメンバーにするべき質問を生成する生成ステップと、生成した前記質問を前記メンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する回答取得ステップと、前記取得した回答に基づき、セキュリティポリシーを構築する構築ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【0037】

このような構成によって、質問に基づきセキュリティポリシーのドラフトを構築できる。

【0038】

また、本発明は、前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【 0 0 3 9 】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【 0 0 4 0 】

また、本発明は、前記回答取得ステップは、前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すステップと、の少なくとも1のステップを含むことを特徴とするセキュリティポリシー構築方法である。

【 0 0 4 1 】

このような構成によって、複数のエンジニアで分散してインタビューをした場合に、その回答のを整合性をとり、インタビュー結果を統合可能である。

【 0 0 4 2 】

また、本発明は、前記構築ステップは、前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、の3レベルのセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【 0 0 4 3 】

3レベルのセキュリティポリシーが構築されるため、階層的なセキュリティポリシーを得ることができる。ここで、前記コーポレートレベルポリシーの基準に基づき実行するための手段とは、ハードウェア・ソフトウェアだけでなく、それらを利用する際の運用ルール等も含む。

【 0 0 4 4 】

また、本発明は、前記コーポレートレベルポリシーは、前記団体全体の情報セキュリティシステムの基準を記述し、前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述することを特徴とするセキュリティポリシー構築方法である。

【 0 0 4 5 】

このような構成によって団体全体のセキュリティポリシーと、個別の機器のセキュリティポリシーとを明確にすることができる。ここで、機器とは、ネットワーク、ホスト、アプリケーション、を含む概念である。

【 0 0 4 6 】

また、本発明は、前記プロダクトレベルポリシーは、自然言語で情報セキュリティシステムを構成する各構成装置の設定を記述する第 1 レベルと、特定商品の特定言語で情報セキュリティシステムを構成する各構成装置の設定を記述する第 2 レベルと、の 2 種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築方法である。

【 0 0 4 7 】

このように、自然言語によるプロダクトレベルポリシーによって、人間がセキュリティポリシーを理解することができ、さらに特定言語で記述されたプロダクトレベルポリシーによって各装置の設定が容易になる。ここで、構成装置は、情報セキュリティシステムを構成するハードウェア・ソフトウェアを含むものである。

【 0 0 4 8 】

また、本発明は、前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップ、を含み、前記分析ステップは、前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、前記回答群によって得られた団体の情報システムと、団体の実際の情報システムとの間に差異があるか否かを調査する差異検出ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【 0 0 4 9 】

このような構成によって、矛盾点や、差異を効率的に検出することができる。

【 0 0 5 0 】

また、本発明は、前記調査した差異の対策をその優先度と共に立てる対策ステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【 0 0 5 1 】

対策がその優先度と共に立てられるため、情報セキュリティの構築計画を立案するのが容易になる。

【 0 0 5 2 】

また、本発明は、団体に属するメンバーにするべき質問を生成する質問生成手段と、前記生成した質問に対する回答を保管する記憶手段と、前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、を含むことを特徴とするセキュリティポリシー構築装置である。

【 0 0 5 3 】

このような構成によれば、メンバーに対する質問が生成されるため、質問作業が容易になる。なお、メンバーとは、その団体の情報システムに関連する個人を意味する。たとえば、従業員だけでなく、パートタイムワーカーや、関連会社の社員等も含まれる。

【 0 0 5 4 】

また、本発明は、前記質問生成手段は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするセキュリティポリシー構築装置である。

【 0 0 5 5 】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【 0 0 5 6 】

また、本発明は、前記回答保管手段は、前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、又は、前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納し、又は、前記

取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を推定し、推定した回答を示すことを特徴とするセキュリティポリシー構築装置である。

【 0 0 5 7 】

このような構成によって、複数のエンジニアで分散してインタビューをした場合に、整合性をとり、統合可能である。

【 0 0 5 8 】

また、本発明は、前記構築手段は、前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、の3レベルのセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【 0 0 5 9 】

3レベルのセキュリティポリシーが構築されるため、階層的なセキュリティポリシーを得ることができる。ここで、前記コーポレートレベルポリシーの基準に基づき実行するための手段とは、ハードウェア・ソフトウェアだけでなく、それらを利用する際の運用ルール等も含む。

【 0 0 6 0 】

また、本発明は、前記コーポレートレベルポリシーは、前記団体全体の情報セキュリティシステムの基準を記述し、前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述することを特徴とするセキュリティポリシー構築装置である。

【 0 0 6 1 】

このような構成によって団体全体のセキュリティポリシーと、個別の機器のセキュリティポリシーとを明確にすることができる。ここで、機器とは、ネットワーク、ホスト、アプリケーション、を含む概念である。

【 0 0 6 2 】

また、本発明は、前記プロダクトレベルポリシーは、自然言語で情報セキュリティシステムを構成する各装置の設定を記述する第1レベルと、特定商品の特定言語で情報セキュリティシステムを構成する各装置の設定を記述する第2レベルと、の2種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築装置である。

【0063】

このように、第1レベルのプロダクトレベルポリシーによって、人間がセキュリティポリシーを理解することができ、さらに第2レベルのプロダクトレベルポリシーによって各装置の設定が容易になる。ここで、構成装置は、情報セキュリティシステムを構成するハードウェア・ソフトウェアを含む。

【0064】

また、本発明は、団体のセキュリティ状況を評価する評価方法において、前記団体に属するメンバーにすべき質問を生成する質問生成ステップと、前記生成した質問を前記メンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する回答取得ステップと、前記取得した回答に基づき、セキュリティ状況を評価するセキュリティ状況評価ステップと、を含むことを特徴とする評価方法である。

【0065】

このような構成によって、質問に対する回答に基づき、団体のセキュリティの状況を知ることが可能である。

【0066】

また、本発明は、前記質問生成ステップは、被質問者の職務内容に基づき、前記被質問者にすべき質問を生成することを特徴とする評価方法である。

【0067】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【0068】

また、本発明は、前記回答保管ステップは、前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得

した回答とを統合し、単一の被質問者の回答として記憶手段中に保管することを特徴とする評価方法である。

【 0 0 6 9 】

このような構成によって、複数のエンジニアで分散してインタビューをした場合に、その回答のを整合性をとり、インタビュー結果を統合可能である。

【 0 0 7 0 】

また、本発明は、前記セキュリティ状況の評価は、前記団体のセキュリティの評価と、前記団体が属する産業分野に含まれる他の団体のセキュリティの評価の平均と、前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの評価の最高値と、を含むことを特徴とする評価方法である。

【 0 0 7 1 】

このような構成によって、その団体を他社と比較して評価することが可能である。また、理論上の最高値が示されるので、経営者が、指標とする目標を定めやすくなる。

【 0 0 7 2 】

また、本発明は、前記セキュリティ状況の評価は、セキュリティに対する理解と姿勢、前記団体のセキュリティ体制、不測事態対応、セキュリティに関する予算化、セキュリティ改善措置、の各項目に関する点数を含むことを特徴とする評価方法である。

【 0 0 7 3 】

このような構成によって、団体の情報セキュリティの評価を、経営者にとっての概念レベルとしてのセキュリティの考え方を、項目別に知ることが可能である。

【 0 0 7 4 】

また、本発明は、団体のセキュリティの状況を評価する評価装置において、団体に属するメンバーにするべき質問を出力する出力手段と、前記出力した質問に対する回答を保管する記憶手段と、前記出力した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、前記保管した回答に基づき、団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成

度作成手段と、を含むことを特徴とする評価装置である。

【0075】

このような構成によって、生成された質問をメンバーに行い、質問に対する回答に基づき、団体のセキュリティの状況を知ることが可能である。

【0076】

また、本発明は、前記回答保管手段は、前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として前記記憶手段中に保管することを特徴とする評価装置である。

【0077】

このような構成によって、複数人で質問をした場合に、得られた回答を統合することが可能である。

【0078】

また、本発明は、前記セキュリティ完成度報告書は、前記団体のセキュリティの完成度と、前記団体が属する産業分野に含まれる他の団体のセキュリティの完成度の平均と、前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの完成度の最高値と、を含むことを特徴とする評価装置である。

【0079】

このような構成によって、その団体を他社の平均と比較して評価することが可能である。また、理論上の最高値が示されるので、目標を設定することが容易となる。

【0080】

また、本発明は、前記セキュリティ完成度報告書は、セキュリティに対する理解と姿勢、団体のセキュリティ体制、不測事態対応、セキュリティに関する予算化、セキュリティ改善措置、の各項目に関する点数を含むことを特徴とする評価装置である。

【0081】

このような構成によって、団体の情報セキュリティの評価を、経営者にとって

の概念レベルとしてのセキュリティの考え方を、項目別に知ることが可能である。

【 0 0 8 2 】

また、本発明は、セキュリティポリシーと、団体の情報システムとの差異を分析する分析装置において、団体のメンバーに質問をすることによって得られた回答群に含まれる個々の回答の間に矛盾があるか否か検査する矛盾検査手段と、前記検査した矛盾に関する情報を出力する矛盾出力手段と、を含むことを特徴とする分析装置である。

【 0 0 8 3 】

このような構成によって、回答群中に含まれる矛盾を知ることが可能である。

【 0 0 8 4 】

また、本発明は、前記矛盾に関する情報に基づき、前記回答群中の矛盾点を指摘する指摘手段と、前記指摘手段が指摘した矛盾点が解決された回答群に基づき、団体の情報システムの構成を仮想的に構築する構築手段と、前記仮想的に構築した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、を含むことを特徴とする分析装置である。

【 0 0 8 5 】

このような構成によって、セキュリティポリシーと団体の実態との差異を知ることができる。

【 0 0 8 6 】

また、本発明は、前記団体の情報システムを調査し、前記情報システムの構成を入力する実システム入力手段と、前記情報システムの構成によって、前記仮想的に構成した情報システムをプルーフし、プルーフ後の前記仮想的に構成した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、を含むことを特徴とする分析装置である。

【 0 0 8 7 】

このような構成によって、実際の調査によってプルーフした情報システムとセキュリティポリシーの比較を行っているので、両者の差異をより正確に分析することができる。

【 0 0 8 8 】

以下、実施の形態 2 に関する発明である。

【 0 0 8 9 】

本発明は、上記課題を解決するために、前記生成ステップは、前記団体の業種に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【 0 0 9 0 】

また、本発明は、前記質問生成手段は、前記団体の業種に基づき、被質問者にすべき質問を生成することを特徴とするセキュリティポリシー構築装置である。

【 0 0 9 1 】

これらの発明によれば、団体の業種を考慮しているため、その業種に対応したセキュリティポリシーを構築することができる。

【 0 0 9 2 】

以下、実施の形態 3 に関する発明である。

【 0 0 9 3 】

本発明は、前記構築ステップは、特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【 0 0 9 4 】

また、本発明は、前記構築手段は、特定の業種向けの勧告又は規定の項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【 0 0 9 5 】

このような構成によれば、特定の業種に関しては汎用的なグローバルガイドラインより詳細な項目についてセキュリティポリシーを構築することが可能である。

【 0 0 9 6 】

以下、実施の形態 4 に関する発明である。

【0097】

本発明は、前記構築ステップは、利用者が指示した1種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【0098】

また、本発明は、前記構築手段は、利用者が指示した1種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【0099】

これらの発明の構成によれば、用いるセキュリティポリシーを利用者に選択することができる。

【0100】

また、本発明は、前記生成ステップは、利用者が指示した1種類又は複数種類のグローバルガイドラインに基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【0101】

同様に、本発明は、前記質問生成手段は、利用者が指示した1種類又は複数種類のグローバルガイドラインに基づき、被質問者にすべき質問を生成することを特徴とするセキュリティポリシー構築装置である。

【0102】

このような構成によれば、利用者の指示するグローバルガイドラインに応じた質問がなされるため、効率的な質問をすることができる。

【0103】

以下、実施の形態6に関する発明である。

【0104】

本発明は、前記構築ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【0105】

また、本発明は、前記構築手段は、利用者が指示したセキュリティポリシーの強度指標に基づき、セキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【 0 1 0 6 】

これらの発明の構成によれば、使用者が「強度指標」を用いてセキュリティポリシーの強度を自由に指示することが可能である。

【 0 1 0 7 】

また、本発明は、前記生成ステップは、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【 0 1 0 8 】

同様に、本発明は、前記質問生成手段は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築装置である。

【 0 1 0 9 】

このような構成によれば、利用者が指示する強度に応じて質問が作成される。後述するように、強度を強く指示すれば一般に質問の個数が増え、細かい事項に関する質問も生成される。強度を弱く指示すれば一般に質問の個数は減り、その内容も細かな内容ではなくなる。強度に応じた質問が生成されるため、より効率的な質問を行うことができる。

【 0 1 1 0 】

次に、本発明は、セキュリティポリシーの強度を調整するセキュリティポリシー強度調整方法において、前記セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないと判断されたルールを、前記強度指標に合致したルールに置き換える強度調整ステップと、前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力ステップと、を含むことを特徴とするセキュリティポリシー強度調整方法である。

【 0 1 1 1 】

また、本発明は、セキュリティポリシーの強度を調整するセキュリティポリシー強度調整装置において、前記セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手段と、前記強度指標に合致していたルールと、前記強度調整手段が置き換えたルールとを、合成して出力する合成出力手段と、を含むことを特徴とするセキュリティポリシー強度調整装置である。

【 0 1 1 2 】

これらの発明の構成によれば、利用者が強度指標で指示した強度になるように、セキュリティポリシーの強度の調整を行うことができる。

【 0 1 1 3 】

以下、実施の形態 6 に関する発明である。

【 0 1 1 4 】

本発明は、所定の団体のセキュリティポリシーを構築する方法において、前記団体のセキュリティポリシーを構築するために必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する生成ステップと、生成した前記質問をメンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する取得ステップと、前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築ステップと、を含み、前記構築ステップは、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【 0 1 1 5 】

このような構成によれば、利用者の指示する範囲のセキュリティポリシーが得られる。

【 0 1 1 6 】

また、本発明は、前記生成ステップは、利用者が指示した構築範囲に関する質問を生成することを特徴とするセキュリティポリシー構築方法である。

【 0 1 1 7 】

このような構成によれば、利用者が指示する範囲に関する質問のみが生成されるため、範囲とは関係のない質問をしてしまうことがない。

【 0 1 1 8 】

また、本発明は、所定の団体のセキュリティポリシーを構築するセキュリティポリシー構築装置において、前記団体のセキュリティポリシーを構築するために必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する質問生成手段と、前記生成した質問に対する回答を保管する記憶手段と、前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、を含み、前記構築手段は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【 0 1 1 9 】

このような構成によれば、利用者の指示する範囲のセキュリティポリシーが得られる。

【 0 1 2 0 】

また、本発明は、前記質問生成手段は、利用者が指示した構築範囲に関する質問を生成することを特徴とするセキュリティポリシー構築装置である。

【 0 1 2 1 】

このような構成によれば、利用者が指示する範囲に関する質問のみが生成されるため、範囲とは関係のない質問をしてしまうことがない。

【 0 1 2 2 】

以下、実施の形態 7 に関する発明である。

【 0 1 2 3 】

実施の形態 7 では、今まで述べた種々の動作をコンピュータに実行させるプログラム及びそのプログラムが記録されている記録媒体（ハードディスク等）が示されている。したがって、これらのプログラム及びプログラムを記録した記録媒体の作用は、今まで述べた発明と同様である。

【 0 1 2 4 】

まず、本発明は、所定の団体のセキュリティポリシーを構築するのに必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する

質問生成手順と、前記生成した質問に対する回答を入力し、記憶手段に格納する回答保管手順と、前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【 0 1 2 5 】

また、本発明は、前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にすべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体である。

【 0 1 2 6 】

また、本発明は、前記回答保管手順は、前記入力した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、又は、前記入力した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、最終的な回答を推定し、推定した回答を示すことを特徴とするコンピュータ読み取り可能な記録媒体である。

【 0 1 2 7 】

また、本発明は、前記質問生成手順は、前記団体の業種に基づき、前記被質問者にすべき質問を生成することを特徴とするコンピュータ読み取り可能な記録媒体である。

【 0 1 2 8 】

また、本発明は、前記構築手順は、利用者が指示した 1 種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを特徴とするコンピュータ読み取り可能な記録媒体である。

【 0 1 2 9 】

また、本発明は、前記質問生成手順は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするコンピュータ読み

取り可能な記録媒体である。

【 0 1 3 0 】

また、本発明は、前記構築手順は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするコンピュータ読み取り可能な記録媒体である。

【 0 1 3 1 】

また、本発明は、所定の団体のセキュリティの完成度を評価するために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問を出力する質問出力手順と、前記出力した質問に対する回答を入力し、記憶手段に格納する回答保管手順と、前記記憶手段に保管した前記回答に基づき、前記団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【 0 1 3 2 】

また、本発明は、所定の団体のセキュリティポリシーと、前記団体の情報システムとの差異を知るために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問に対する回答群中の個々の回答間に矛盾があるか否かを検査する矛盾検査手順と、前記検査した矛盾に関する情報を出力する矛盾出力手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【 0 1 3 3 】

また、本発明は、前記矛盾に関する情報に基づき、前記回答群の整合をとり、矛盾点を解決した回答群を生成する整合手順と、前記整合した後の回答群に基づき、前記団体の情報システムの構成を仮想的に構築する構築手順と、前記仮想的に構築した情報システムの構成と、前記セキュリティポリシーとを比較し、両者の差異を出力する差異出力手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【 0 1 3 4 】

また、本発明は、セキュリティポリシー中の個々のルールであって、利用者が

指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手順と、前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力手順と、をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【 0 1 3 5 】

以上の発明が、記録媒体に関する発明である。次に、プログラムに関する発明を示す。

【 0 1 3 6 】

本発明は、所定の団体のセキュリティポリシーを構築するのに必要な事項に関する質問であって、前記団体に属するメンバーにするべき質問を生成する質問生成手順と、前記生成した質問に対する回答を入力し、記憶手段に保管する回答保管手順と、前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手順と、をコンピュータに実行させるためのプログラムである。

【 0 1 3 7 】

また、本発明は、前記質問生成手順は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするプログラムである。

【 0 1 3 8 】

また、本発明は、前記回答保管手順は、前記入力した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、又は、前記入力した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、最終的な回答を推定し、推定した回答を示すことを特徴とするプログラムである。

【 0 1 3 9 】

また、本発明は、前記質問生成手順は、前記団体の業種に基づき、前記被質問者にするべき質問を生成することを特徴とするプログラムである。

【 0 1 4 0 】

また、本発明は、前記構築手順は、利用者が指示した 1 種類又は複数種類のグローバルガイドラインの項目に基づき、セキュリティポリシーを構築することを

特徴とするプログラムである。

【 0 1 4 1 】

また、本発明は、前記質問生成手順は、利用者が指示したセキュリティポリシーの強度指標に基づき、前記質問を生成することを特徴とするプログラムである。

【 0 1 4 2 】

また、本発明は、前記構築手順は、利用者が指示した構築範囲のセキュリティポリシーを構築することを特徴とするプログラムである。

【 0 1 4 3 】

また、本発明は、所定の団体のセキュリティの完成度を評価するために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問を出力する質問出力手順と、前記出力した質問に対する回答を入力し、記憶手段に保管する回答保管手順と、前記記憶手段に保管した前記回答に基づき、前記団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手順と、をコンピュータに実行させるためのプログラムである。

【 0 1 4 4 】

また、本発明は、所定の団体のセキュリティポリシーと、前記団体の情報システムとの差異を知るために必要な事項に関する質問であって、前記団体のメンバーに対して行う質問に対する回答群中の個々の回答間に矛盾があるか否かを検査する矛盾検査手順と、前記検査した矛盾に関する情報を出力する矛盾出力手順と、をコンピュータに実行させるためのプログラムである。

【 0 1 4 5 】

また、本発明は、前記矛盾に関する情報に基づき、前記回答群の整合をとり、矛盾点を解決した回答群を生成する整合手順と、前記整合した後の回答群に基づき、前記団体の情報システムの構成を仮想的に構築する構築手順と、前記仮想的に構築した情報システムの構成と、前記セキュリティポリシーとを比較し、両者の差異を出力する差異出力手順と、をコンピュータに実行させるためのプログラムである。

【 0 1 4 6 】

また、本発明は、セキュリティポリシー中の個々のルールであって、利用者が指定した強度指標に合致していないルールを、前記強度指標に合致したルールに置き換える強度調整手順と、前記強度指標に合致していたルールと、前記強度調整ステップにおいて置き換えられたルールとを、合成して出力する合成出力手順と、をコンピュータに実行させるためのプログラムである。

【0147】

【発明の実施の形態】

以下、本発明の好適な実施の形態を図面に基づいて説明する。

【0148】

実施の形態1

ある団体に対して行うセキュリティポリシーの構築からそのメンテナンスに至る一連の作業を含むビジネスモデルについて説明する。このビジネスモデルはシステムエンジニアが所定のエキスパートシステムを用いて実行することが好ましい。

【0149】

本実施の形態1におけるビジネスモデルの原理をまず説明する。図1には、このビジネスモデルの原理を表すフローチャートが示されている。この図に示すように、本ビジネスモデルは、基本的には6個のステップから構成される。

【0150】

- ステップ1 セキュリティ完成度評価
- ステップ2 セキュリティポリシードラフト構築
- ステップ3 システム及びその運用の実査・分析
- ステップ4 ポリシー調整・ルール調整
- ステップ5 プライオリティプランニング
- ステップ6 セキュリティ強化策実行

このような6段階のステップからなるセキュリティ構築手法によれば、最初はインタビューベースのセキュリティポリシーのドラフトを構築し、必要に応じ、団体の実態との再調整を行い、段階的にセキュリティポリシーを完成していくので、各団体のスケジュールや予算に合わせてセキュリティポリシーを構築するこ

とが可能である。

【0151】

ステップ1は、団体の情報セキュリティの現状を評価するステップである。この評価によって、団体は自社の経営者レベルの指標を得ることによって、情報セキュリティの現状を知ることができる。

【0152】

ステップ2は、団体のメンバーに対して質問をすることによって簡易にセキュリティポリシーのドラフトを作成するステップである。単にインタビューによってセキュリティポリシーのドラフトを作成しているので、安価にセキュリティポリシーを作成することができる。

【0153】

ステップ3は、仮想システムと、団体の実態との相違を検討するステップである。仮想システムは質問に対する回答にのみ基づき作成されているので、実態との相違が生じる場合があるからである。

【0154】

ステップ4は、差異に基づいて、セキュリティポリシーを調整又は導入済みのセキュリティ商品のルールを調整するステップである。

【0155】

ステップ5は、今後の情報セキュリティ計画を、各手段や対策を採用する優先度も含めて構築するステップである。

【0156】

ステップ6は、この計画に基づいて、必要なセキュリティ保護対策を実施するステップである。

【0157】

以上のように段階的にセキュリティポリシーの構築を行っているため、各団体の予算や考え方等の実状に合わせたセキュリティポリシーの構築が可能である。

【0158】

たとえば、会社の考え方や、予算によっては、セキュリティポリシーのドラフトで十分な場合もあろう。また、プライオリティプランニングによれば、将来の

計画がわかるため、団体の予算を立てやすくなるというメリットがある。

【0159】

特に、本ビジネスモデルについて中心的なステップは、ステップ2～ステップ4である。ステップ2においてドラフトを作成し、ステップ3において実態との差異を分析し、ステップ4においてセキュリティポリシー又は導入済みのセキュリティ商品の調整を行う。少なくともこれらステップ2～ステップ4を含むビジネスモデルであれば、セキュリティポリシーの構築をシステムティックに行うことができ、従来の経験と勘に頼る手法に比べて、生産性及び品質を高めることが可能である。

【0160】

また、このような段階的なセキュリティポリシーの構築を実現するために、本実施の形態1では、種々のエキスパートシステムを使用している。

【0161】

以下、エキスパートシステムの利用方法も含めて、ステップ1～ステップ6の各ステップを順に説明する。

【0162】

A. ステップ1：セキュリティ完成度評価

このステップでは、団体の現在の情報セキュリティに関する客観的な評価を行う。このような評価を行うことによって、セキュリティに関する団体のランク付けを行うことが可能である。なお、具体的には、上記評価は、セキュリティ完成度評価書を作成することによって実行される。

【0163】

本実施の形態1では、米国カーネギーメロン大学のSoftware Capability Maturity Modelに基づき、セキュリティ完成度評価を行う。このModelでは、5個の項目に対して定量的評価を行う。すなわち、点数を与えるのである。

【0164】

5個の項目は、以下の通りである。

【0165】

a. 情報セキュリティに対する管理者の理解と姿勢

- b. 団体のセキュリティ状況
- c. 不測事態対応
- d. セキュリティに関する予算化
- e. セキュリティ改善措置

ここで、不測事態とは、情報セキュリティを脅かす事象をいう。たとえば、盗聴行為、機器の故障等である。これらの不測事態に対応できる体制にあるか否かを表すのが上記 c. 不測事態対応である。また、d. 予算化とは、情報セキュリティのために予算が十分にとられているか否かを表す。また、e. セキュリティ改善措置とは、セキュリティの改善の予定や計画がどの程度立てられているか、を表す。

【 0 1 6 6 】

本実施の形態 1 では、このような 5 個の項目に関する点数付けを含む完成度評価書を作成することによって、団体の経営者の指標、セキュリティに対する取り組みに関する意識レベルの客観的な評価を知ることができる。

【 0 1 6 7 】

具体的なセキュリティ完成度評価書の作成手法について説明する。

【 0 1 6 8 】

本実施の形態 1 では、団体に属する経営者に質問をし、その回答に基づいて、完成度評価書を作成する。具体的には、図 2 に示すような評価装置 1 0 を用いて、質問の生成、回答の収集、セキュリティ完成度評価書の作成等を実行している。また、評価書の作成作業の動作を表すフローチャートが図 3 に示されている。この図 3 に示されているフローチャートは、図 1 におけるステップ S 1 - 1 をより詳細に表したフローチャートである。

【 0 1 6 9 】

まず、図 2 に示すように、評価装置 1 0 は、被質問者に行うべき質問を出力する質問出力手段 1 2 を備えている。

【 0 1 7 0 】

記憶手段 1 4 には、あらかじめ多種多様な質問が格納されており、被質問者に必要な質問が質問出力手段 1 2 によって抽出されるのである。

【0171】

また、評価装置10は、回答保管手段16を備えている。上記のようにして生成した質問を団体に属する経営者に提示して得られた回答は、この回答保管手段16に供給される。回答保管手段16は、回答を記憶手段14に保管する。

【0172】

本実施の形態1において特徴的なことは、回答保管手段16が回答の統合機能を有していることである。この統合機能とは、質問を複数人のシステムエンジニアが行った場合に、その回答を1個のデータベースにまとめて記憶手段14に保管する機能である。質問をするべき経営者が多数いる場合には、複数人のシステムエンジニアが分担してインタビュー質問を行った方が迅速に質問に対する回答を得ることができる。このように質問を分担して実行した場合に、その結果は複数のコンピュータ上にそれぞれ蓄積される。したがって、これらの結果を統合する必要があるのである。

【0173】

もちろん、ある1人の経営者に対する質問や回答が一度にできず、複数回に分けて行われた場合に、それらの結果を統合するためにも利用可能である。

【0174】

また、評価装置10は、セキュリティ完成度報告書の作成を行うセキュリティ完成度作成手段18を備えている。このセキュリティ完成度作成手段18は、記憶手段14に保管されている回答群に基づきその団体の情報セキュリティに関する評価書であるセキュリティ完成度報告書を作成する。

【0175】

この評価装置10はいわゆるエキスパートシステムである。

【0176】

特に、上述したように、本実施の形態1では、収集した回答を統合する機能等を備える評価装置10を採用している。したがって、セキュリティ完成度評価書を効率よくしかも精密に作成することが可能である。

【0177】

次に、図3のフローチャートに基づき、セキュリティ完成度評価書の作成動作

について説明する。

【 0 1 7 8 】

まず、ステップ S 3 - 1 においては、質問出力手段 1 2 が、その経営者に対して行う質問を出力する。

【 0 1 7 9 】

そして、ステップ S 3 - 2 において、システムエンジニアは得られた質問を経営者に対して行う。

【 0 1 8 0 】

ステップ S 3 - 3 においては、質問に対する回答を経営者から得て、評価装置 1 0 の回答保管手段 1 6 に供給する。

【 0 1 8 1 】

さて、ステップ S 3 - 4 においては、セキュリティ完成度作成手段 1 8 が記憶手段 1 4 に格納された回答群に基づいて、上記の 5 項目に関するスコア（点数）を含むセキュリティ完成度評価書を作成する。

【 0 1 8 2 】

以上のようにして、評価装置 1 0 を用いて、セキュリティ完成度評価書が作成される。

【 0 1 8 3 】

業界標準との比較

セキュリティ完成度評価書には、上述したように、5 個の項目に関するスコア（点数）が示される。

【 0 1 8 4 】

特に、本実施の形態 1 において特徴的なことは、その団体の属する業界における全団体の平均的なスコア及び最高のスコアが併せて表示されることである。ここで、最高のスコアとは、その業界に含まれる団体であれば達成できるであろう最高のスコア（理論値）である。

【 0 1 8 5 】

これによって、その団体の情報セキュリティに対する取り組みが、その業界の中でどの程度の位置にいるかを容易に知ることが可能である。なお、このような

業界の平均値や最高値は、記憶手段14にあらかじめ格納してある。さらに、平均値は、セキュリティ完成度評価を実行して、定期的に更新される。

【0186】

セキュリティ実装の経緯報告

本実施の形態1では、セキュリティ完成度評価書は、セキュリティポリシーの構築を行う前に団体の経営者の意識を調査する趣旨で作成している。しかし、情報セキュリティの対策を順次実行していく途中段階で適宜このセキュリティ完成度報告書を作成すれば、情報セキュリティ対策の進捗の程度を知ることが可能である。したがって、このセキュリティ完成度報告書の作成ステップは、セキュリティ実装の経緯報告としての性格も有する。

【0187】

なお、本実施の形態1の評価装置10では、質問や回答などがすべて記憶手段14に格納されているが、それぞれ専用の別個の記憶手段に格納してもかまわない。

【0188】

B. ステップ2：セキュリティポリシードラフト構築

このステップでは、その団体のセキュリティポリシーの簡単なドラフトを構築する。このドラフトは、団体に属するメンバーに質問をし、その回答に基づき構築するセキュリティポリシーである。したがって、団体の実際の情報システムの調査を行っていないため、迅速にセキュリティポリシーの構築を行うことができる。

【0189】

標準的なセキュリティポリシーを構築するための基本的な項目、内容が国際的なガイドラインとして種々知られている。これらをグローバルガイドラインと呼ぶ。本実施の形態1では、これらグローバルガイドライン中の原則を、適宜取り出し、組み合わせることによって、セキュリティポリシーのドラフトを構築する。

【0190】

本実施の形態1では、セキュリティポリシードラフト構築装置20を利用して

セキュリティポリシーのドラフトを構築している。このセキュリティポリシードラフト構築装置 20 の構成ブロック図が図 4 に示されている。

【0191】

セキュリティポリシードラフト構築装置 20 は、図 4 に示すように、被質問者の職務内容に基づいて、行うべき質問を生成する質問生成手段 22 を備えている。このように職務内容に基づいて、質問を変更するのは、上記評価装置 10 の質問生成手段 12 と同様に、有意義な回答を得るためである。

【0192】

また、図 2 の記憶手段 14 と同様に、セキュリティポリシードラフト構築装置 20 内の記憶手段 24 にも、多種多様な質問があらかじめ格納されている。そして、質問生成手段 22 が、メンバーの職務内容に応じて適切な質問を記憶手段 24 から抽出するのである。

【0193】

また、セキュリティポリシードラフト構築装置 20 は、回答保管手段 26 を備えている。この回答保管手段 26 も、上記回答保管手段 16 と同様に回答を記憶手段 24 に保管する。また、回答保管手段 26 は、回答の統合機能を有している。

【0194】

統合機能

統合機能は、以下のような機能を含んでいる。

【0195】

(1) 複数のエンジニアが、分散してメンバーにインタビューを行い、インタビュー結果である回答を収集し、一つのデータベースにまとめる。たとえば、ある 1 人のメンバーに複数のエンジニアがインタビューをした場合には、それらの回答は 1 のデータベースに統合される。また、たとえば、同種類（たとえばネットワーク）に関する一連の質問を、複数のメンバーにした場合、それらの回答を統合して 1 のデータベースに組み込む。

【0196】

(2) インタビューにおいては同一の質問が異なるメンバーになされる場合が

ある。その結果、回答に矛盾が生じる場合も考えられる。この矛盾を解決するためには、2つの手法がある。第1の手法は、再インタビューである。矛盾点に関し、回答者に言い間違い等があった場合には、再インタビュー又は実査（又はそれら双方）を実行することにより矛盾点を解決できると考えられる。第2の手法は、タイプ（職務内容）によるウェイト付け（重み付け）で、回答を定める方法である。

【0197】

本実施の形態1においては、利用者はこの第1の手法と第2の手法を自由に選択することができる。

【0198】

また、セキュリティポリシードラフト構築装置20は、セキュリティポリシーのドラフトを構築するドラフト構築手段28を備えている。このドラフト構築手段28は、記憶手段24に保管されている回答群に基づきそのセキュリティポリシーのドラフトを作成する。

【0199】

このセキュリティポリシードラフト構築装置20も、評価装置10と同様にいわゆるエキスパートシステムであり、実際には上記各手段は、コンピュータ上で動作するソフトウェアによって実現することが好ましい。

【0200】

次に、図5のフローチャートに基づき、セキュリティポリシーのドラフトを構築する動作を説明する。図5には、セキュリティポリシードラフト構築装置20を用いてセキュリティポリシーのドラフトを構築する動作を表すフローチャートが示されている。

【0201】

まず、ステップS5-1においては、被質問者であるメンバーの職務内容を質問生成手段22に供給し、そのメンバーに対して行う質問を生成する。

【0202】

本実施の形態1においては、このようにそのメンバーの職務内容によって生成する質問が決定される。その結果、被質問者に対して行うべき適切な質問を生成

することが可能である。

【0203】

メンバーの職務内容によって決定されるのは、質問群のいわばコースである。各コースにおいて出される実際の質問は、メンバーの回答内容によって変更される。たとえば、VPNを使用しているかという質問に対して、使用していないと回答すれば、VPNの詳細に関する質問はスキップされる。しかし、VPNを使用していると回答した場合には、その回答をしたメンバーには、VPNの詳細に関する質問がなされる。

【0204】

このような制御は、いわゆる知識ベースのエキスパートシステムを利用して実行される。

【0205】

ステップS5-2において、生成した質問をメンバーに対して行う。

【0206】

ステップS5-3においては、質問に対する回答をメンバーから得て、セキュリティポリシードラフト構築装置20の回答保管手段26に入力する。入力作業は質問者自身が行うのが好ましい。もちろん、質問を受ける各メンバーがポリシードラフト構築装置20の画面に向かって、表示される質問に答えるような形態を採用してもかまわない。回答保管手段26は上述のように統合機能を有しており、複数の質問者が取得してきた回答を統合して、記憶手段24に格納する。

【0207】

ステップS5-4においては、ドラフト構築手段28が記憶手段24に格納された回答群に基づいて、グローバルガイドライン中の原則を種々組み合わせてセキュリティポリシーを構築する。

【0208】

以上のようにして、セキュリティポリシードラフト構築装置20を用いて、セキュリティポリシーのドラフトが作成される。

【0209】

なお、本実施の形態1では、エグゼクティブレベルポリシー、コーポレートレ

ベルポリシー、プロダクトレベルポリシーの3レベルのセキュリティポリシー（のドラフト）が構築される。これら3レベルに関する説明は、B-5章において後述する。

【0210】

B-1：質問（インタビュー）の内容

以下、質問（以下、インタビューとも呼ぶ）の内容について説明する。

【0211】

インタビュー大項目は、以下の通りである。

【0212】

1. 団体
2. ネットワーク
3. サーバとホスト
4. アプリケーションとデータベース
5. 重要性の高いセキュリティ項目
6. その他のセキュリティ項目

以下、各項目を説明する。

【0213】

（1）団体

項目「団体」では、団体の概要、体制に関するインタビューが実行される。このインタビュー質問の回答から、情報セキュリティの管理体制、ポリシーの原則、脆弱性分析（差異分析）等を導くことが可能である。

【0214】

項目「団体」には、さらに小項目として、以下の項目が含まれている。

【0215】

1. 1 管理体制
1. 2 従業員
1. 3 会社概要
1. 4 ベンダー
1. 5 顧客

- 1. 6 コンサルタント
- 1. 7 外部委託
- 1. 8 アプリケーション
- 1. 9 ネットワーク
- 1. 10 セキュリティプロファイル
- 1. 11 業種
- 1. 12 団体ポリシー

ただし、職務内容によって質問項目が異なる。たとえば、最高経営責任者にはホストについての質問項目はない。このように、本実施の形態1において特徴的なことは、職務によって質問内容が異なることである。これによって、その職務内容に応じた質問をすることができ、効率的なインタビューが可能である。

【0216】

(2) ネットワーク

項目「ネットワーク」では、ネットワークの概要、運用、設定に関するインタビュー質問が実行される。このインタビュー質問の回答から、ネットワークの脆弱性、ネットワークに関するコーポレートレベルポリシー等が導かれる。

【0217】

項目「ネットワーク」には、さらに小項目として、以下の項目が含まれている。

【0218】

- 2. 1 運用環境
- 2. 2 ネットワークのプロパティ
- 2. 3 認証と識別
- 2. 4 監査とログ
- 2. 5 アクセス制御
- 2. 6 変更手続き
- 2. 7 災害復旧とバックアップ
- 2. 8 オペレーションの信頼性
- 2. 9 物理的セキュリティ

2. 10 モデム

2. 11 ワークステーションセキュリティ

(3) サーバとホスト

項目「サーバとホスト」では、ホストの概要、運用、設定に関するインタビュー質問が実行される。このインタビュー質問の回答から、ホストの脆弱性、ホストとサーバに関するコーポレートレベルポリシー等が導かれる。

【0219】

項目「サーバとホスト」には、さらに小項目として、以下の項目が含まれている。

【0220】

3. 1 サーバとホストプロパティ

3. 2 認証と識別

3. 3 監査とログ

3. 4 アクセス制御

3. 5 変更手続き

3. 6 災害復旧とバックアップ

3. 7 オペレーションの信頼性

3. 8 物理的セキュリティ

(4) アプリケーションとデータベース

項目「アプリケーションとデータベース」では、アプリケーションの概要、運用、設定に関するインタビュー質問が実行される。このインタビュー質問の回答から、アプリケーションの脆弱性、アプリケーションに関するコーポレートレベルポリシー等が導かれる。

【0221】

項目「アプリケーションとデータベース」には、さらに小項目として、以下の項目が含まれている。

【0222】

4. 1 アプリケーション、データベースのプロパティ

4. 2 認証と識別

- 4. 3 監査とログ
- 4. 4 アクセス制御
- 4. 5 変更手続き
- 4. 6 災害復旧とバックアップ
- 4. 7 オペレーションの信頼性
- 4. 8 物理的セキュリティ

(5) 重要性の高いセキュリティ項目

項目「重要性の高いセキュリティ項目」では、一般的にファイアーウォールやアクセスコントロールを構築する際に必要な情報に関するインタビュー質問が実行される。このインタビュー質問の回答から、コーポレートレベルポリシー、プロダクトレベルポリシー等が導かれる。項目「重要性の高いセキュリティ項目」に含まれる質問群の多くはコーポレートレベルポリシーやプロダクトレベルポリシーに関する質問であるが、エグゼクティブレベルポリシーに影響を与える質問もある。

【0223】

項目「重要性の高いセキュリティ項目」には、さらに小項目として、以下の項目が含まれている。

【0224】

- 5. 1 ファイアーウォールの管理
- 5. 2 パケットフィルタリング
- 5. 3 NAT（ネットワークアドレス変換）
- 5. 4 SMTPコンテンツフィルタリング
- 5. 5 FTPコンテンツフィルタリング
- 5. 6 HTTPコンテンツフィルタリング
- 5. 7 ログとアラート

(6) その他のセキュリティ項目

項目「その他のセキュリティ項目」では、一般的にVPNを構築する際に必要な情報に関するインタビュー質問が実行される。このインタビュー質問の回答から、コーポレートレベルポリシー、プロダクトレベルポリシー等が導かれる。

【0225】

項目「その他のセキュリティ項目」には、さらに小項目として、以下の項目が含まれている。

【0226】

- 6. 1 VPNのプロパティ
- 6. 2 VPNの管理
- 6. 3 鍵の配布
- 6. 4 ログと監査

B-2 インタビューの形式

インタビューの内容は、上記各項目の通りであるが、インタビューは、記述式や、選択式等種々の形式でなされる。

【0227】

B-3 インタビューの対象者

本実施の形態1のセキュリティポリシードラフト構築装置20は、インタビューの対象となるメンバーによって、質問の内容を変更する。換言すれば、被インタビュー者の職務内容に基づいて、質問の内容を制御しているのである。

【0228】

その結果、被インタビュー者に対して行うべき適切な質問を生成することが可能である。

【0229】

メンバーの職務内容によって決定されるのは、質問群のいわばコースである。各コースにおいて出される質問は、メンバーの回答内容によって変更される。たとえば、VPNを使用しているかという質問に対して、使用していないと回答すれば、VPNの詳細に関する質問はスキップされる。しかし、VPNを使用していると回答した場合には、その回答をしたメンバーには、VPNの詳細に関する質問がなされる。

【0230】

このような制御は、いわゆる知識ベースのエキスパートシステムを利用して実行される。

【 0 2 3 1 】

そのため、実際のインタビューに先立って、被インタビュー者の職務内容をセキュリティポリシー構築装置 2 0 に入力する必要がある。具体的には、以下の項目に関して入力を行う。

【 0 2 3 2 】

* 名前

* 部署名

* 役職

郵便番号

住所

国名

電話番号

E M A I L アドレス

* タイプ

これらの項目の中で、* が頭に付されている項目は必須入力項目である。また、タイプとは、職務内容を表す記号であり、本実施の形態 1 では、図 6 に示される記号を用いて職務内容を表している。簡単に言えば、このタイプはいわゆる職務内容を表す。このタイプに基づき、質問すべき内容が決定される。本実施の形態 1 で取り扱うタイプの一覧表が図 6 に示されている。

【 0 2 3 3 】

なお、実際に被質問者に質問される内容は、質問の回答によって変化する。これはいわゆる知識ベース (Knowledge Base) の動作となる。たとえば、パスワードの有効期限は存在するか？という質問に対し、有効期限はなく無制限だと回答したメンバーに対して、有効期限は何日か？という質問は行わない。これに対して、有効期限はあると答えたメンバーに対しては、有効期限は何日か？という質問が出されうる。

【 0 2 3 4 】

B - 4 管理すべき情報資産

本実施の形態 1 では、セキュリティを確保する情報資産を 5 種類に分類してい

る。その5種類は、ネットワーク、ホスト、アプリケーション、ユーザグループ、その他である。本実施の形態1のセキュリティポリシー構築装置に情報資産を入力する場合には、以下の4項目を入力する。ただし、「ホスト」「ネットワーク」に属するアセットの場合は、さらに2項目、「IPアドレス」「サブネットマスク」を入力する。

【0235】

アセット（資産）ID

*アセットタイプ

*アセット名

詳細

このうち、アセットタイプには5種類のタイプがある。

【0236】

A アプリケーション

H ホスト

N ネットワーク

U ユーザグループ

W その他、URL、ドメイン名、ファイル名

ここで、ユーザグループとは、共通の特徴を有するユーザの論理的な集合をいう。たとえば、会計情報を取り扱い、会計情報を修正、分析、報告するユーザを会計グループと呼ぶ。ユーザグループは1人又は2人以上のユーザから構成される。なお、ユーザとは、その情報資産を使用する人間をいう。

【0237】

B-5 セキュリティポリシードラフトの作成

以上のような質問に対する回答をセキュリティポリシードラフト構築装置20に入力することによって、セキュリティポリシーの構築が実行される。この装置は、いわゆるエキスパートシステムであり、生成した質問に対する回答を入力することによって、セキュリティポリシーを生成し、出力する装置である。このように質問に対する回答を入力することによって何らかのデータを生成する装置は、従来からエキスパートシステムとしてよく知られているため、その詳細は省略

する。

【 0 2 3 8 】

本実施の形態 1 においては、エグゼクティブレベルポリシー、コーポレートレベルポリシー、プロダクトレベルポリシーの 3 レベルのセキュリティポリシーが生成される。したがって、セキュリティポリシーのドラフトに関しても、これら 3 レベルのドラフトが作成される。

【 0 2 3 9 】

(1) エグゼクティブレベルポリシー

エグゼクティブレベルポリシーは、団体のセキュリティに関する「考え方」「方針」を記述したものである。

【 0 2 4 0 】

エグゼクティブレベルポリシーには、たとえば以下の項目が含まれる。

【 0 2 4 1 】

アクセス制御

情報資産に対するアクセス権の管理及び制御は、その情報資産の所有者が制御する必要がある。また、制御は、情報資産が保存又は処理される制御システムが有するアクセス制御の仕組みを使用しなければならない。このアクセス制御では、アクセス権の制御に関するその団体の考え方、方針を記述する。

【 0 2 4 2 】

情報正確性

情報資産の内容を正確にあるがままに維持することは極めて重要な事項である。これは、情報資産は業務上の決定に必要不可欠なものだからである。この情報正確性においては、情報資産の内容の正確性に関する団体の考え方、方針が記述される。

【 0 2 4 3 】

保証

団体は、情報リソースや、セキュリティ対策の適切な安全性を保証するために適切な措置を採用しなければならない。この保証では、そのような措置に関する団体の方針、考え方を記述する。

【 0 2 4 4 】

アカウントビリティ

すべてのシステムはユーザのアクティビティを記録し、分析を可能にしなければならない。各ユーザは、自己の行為に責任を持たなければならない。このアカウントビリティにおいては、各ユーザの自己の責任に関する団体の考え方、方針を記述する。

【 0 2 4 5 】

識別・認証

すべてのユーザは、情報資産の機密性に応じて、適切に識別されなければならない。この識別・認証では、このような識別に関する団体の考え方、方針を記述する。

【 0 2 4 6 】

緊急時対応計画

団体はシステムやネットワークにおける障害に対する適切な対処を保証するために、詳細な計画と手続を作成しなければならない。この緊急時対応計画においては、このような計画と手続に関する団体の考え方、方針を記述する。

【 0 2 4 7 】

セキュリティ認識

従業員及び経営陣は、団体の情報セキュリティの要件を認識すると同時に自己の責任を自覚しなければならない。このセキュリティ認識においては、このような自己の責任に関する団体の考え方、方針を記述する。

【 0 2 4 8 】

情報分類

情報セキュリティは、情報資産を保護するためのものである。したがって、保護すべき対象である情報資産は分類され、各分類にしたがって適切に保護されなければならない。情報分類では、この情報資産に関する団体の考え方、方針を記述する。

【 0 2 4 9 】

職業倫理

ユーザは、定められた行動規範を遵守し、情報資産を取り扱わなければならない。ユーザが方や規則を破り、又は、私的目的のために情報資産を取り扱った場合には、処罰の対象となる。ユーザは処罰の対象となることを認識しなければならない。職業倫理では、ユーザの守るべき行動規範について、団体の考え方、方針を記述する。

【 0 2 5 0 】

文書管理

セキュリティの仕組みはすべて適切に文書化し、必要に応じて参照されなければならない。文書管理では、この文書化に関する団体の考え方、方針を記述する。

【 0 2 5 1 】

調査

団体は障害や侵害が発生した場合には、セキュリティポリシーに沿ってその障害や侵害を調査し、その内容をすべて文書化しなければならない。調査では、このような障害や侵害に関する調査や文書化についての団体の考え方、方針を記述する。

【 0 2 5 2 】

プライバシー

情報資産の使用は関係当事者のプライバシーを保証することを前提としなければならない。プライバシーでは、このプライバシーの保証に関する団体の考え方、方針を記述する。

【 0 2 5 3 】

リスク管理

情報資産の所有者は、潜在するリスクを評価し、適切な制御、又は防衛策を講じなければならない。リスク管理では、このような評価、制御、防衛策に関する団体の考え方、方針を記述する。

【 0 2 5 4 】

検証

団体は、すべてのセキュリティの実装を定期的に検証しなければならない。検

証では、このような検証に関する団体の考え方、方針を記述する。

【0255】

資産評価

団体は情報資産を分析しなければならない。資産評価では、この分析に関する団体の考え方、方針を記述する。

【0256】

セキュリティ管理

団体は、作成したセキュリティポリシーが適切に管理され、変更・修正が必要な場合は、改訂される。セキュリティ管理では、セキュリティポリシーの管理に関する団体の考え方、方針を記述する。

【0257】

(2) コーポレートレベルポリシー

コーポレートレベルポリシーは、団体の情報資産に対してエグゼクティブレベルポリシーの記述を適用し、セキュリティの「運用規定」を記述したものである。この適用は、団体の運用ユニット毎に行われる。運用ユニットとは、情報システムを構成する部分をその作用に基づいてグループ分けしたものである。たとえば、ネットワークや、ホスト、アプリケーション等が、それぞれ運用ユニットである。

【0258】

エグゼクティブレベルポリシーはいわば「憲法（大原則）」を記述したものであるのに対し、コーポレートレベルポリシーは「法律（大原則に基づく規定）」を記述したものである。

【0259】

コーポレートレベルポリシーには、団体全体の情報セキュリティシステムの基準を記述するものと、団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述するものがある。

【0260】

団体に存在する運用ユニット全体に関するポリシーでは、たとえば、以下の規定が記述される。

【 0 2 6 1 】

ネットワーク

このネットワークには、団体ネットワークの全体に対する規定が記述される。

【 0 2 6 2 】

ホスト

このホストには、団体ホストの全体に対する規定が記述される。

【 0 2 6 3 】

アプリケーション

このアプリケーションには、団体アプリケーションの全体に対する規定が記述される。

【 0 2 6 4 】

また、運用ユニットをより細分化した個々のユニットに関する特定のポリシーでは、たとえば、以下のような項目が記述される。

【 0 2 6 5 】

ソフトウェア管理

このソフトウェア管理には、その団体内で用いられる個々のソフトウェアに関するそのソフトウェアの使用やライセンス管理の規定が記述される。

【 0 2 6 6 】

ダイヤルアップ

このダイヤルアップには、その団体内で用いられる個々のダイヤルアップやリモートアクセスサーバに関する規定が記述される。

【 0 2 6 7 】

電子メール

この電子メールには、その団体内で用いられる個々の電子メールの規定が記述される。

【 0 2 6 8 】

ファイアーウォール管理

このファイアーウォールには、その団体内で用いられる個々のファイアーウォールの管理の規定が記述される。

【 0 2 6 9 】

暗号

この暗号には、その団体内で用いられる個々の暗号化の実装規定が記述される。

【 0 2 7 0 】

電子商取引

この電子商取引には、その団体内で用いられる個々の電子商取引の規定が記述される。

【 0 2 7 1 】

ネットワーク

このネットワークには、その団体内で用いられる個々のネットワークの規定が記述される。

【 0 2 7 2 】

ホスト

このホストには、その団体内で用いられる個々のホストの規定が記述される。

【 0 2 7 3 】

アプリケーション

このアプリケーションには、その団体内で用いられる個々のアプリケーションの規定が記述される。

【 0 2 7 4 】

(3) プロダクトレベルポリシー

プロダクトレベルポリシーは、情報資産をどのようなリソース（セキュリティ商品、運用体制）及びその設定を使って保護するか、具体的な「方法」を含む運用手順を記述したものである。上記エグゼクティブレベルポリシーやコーポレートレベルポリシーが、方針や管理面におけるルールを記述しているのに対して、プロダクトレベルポリシーは、ハードウェアやソフトウェアの細部にまでも言及し、エグゼクティブレベルポリシーが提供する「原則」と、コーポレートレベルポリシーが提供する「規定」とに基づいて、具体的にどのように情報資産の保護を実現するかに関する「方法」を提供するものである。したがって、プロダクト

レベルポリシーは、具体的な技術の実装に関する記述を含むものである。

【0275】

このプロダクトレベルポリシーは、ソフトウェアやハードウェアに関する記述を含み、さらに、それらを具体的に運用するルールも記述されている。

【0276】

実際の業務遂行上の理由で、使用する製品が変更される場合もあるかもしれないし、また、機器の故障で代替機器を使用する場合もあるかもしれない。これらの状況に対する責任や製品の基準は、上記エグゼクティブレベルポリシーやコーポレートレベルポリシーが規定する「原則」や「規定」に委ねられている。換言すれば、これらの状況に対する対策等は上記エグゼクティブレベルポリシーやコーポレートレベルポリシーで十分に規定される必要がある。

【0277】

さて、上述したエグゼクティブレベルポリシーは、いわば原則を謳ったものであり、たとえば、「アクセス権は、業務終了と共に抹消されなければならない。」

の如きルールである。

【0278】

また、コーポレートレベルポリシーは、具体的な規定を謳ったものであり、たとえば、「アクセス権はOSで制御されなければならない。」の如きルールである。

【0279】

これに対して、プロダクトレベルポリシーは、具体的な手段を規定するものであり、たとえば、「サーバAのアクセス制御ルールとして部門Bの課長職以上の人間のみしかアクセスできない」や「サーバAのアクセス権の制御は、管理者Xによって管理される。業務上の必要がある者は、管理者Xに依頼し、アクセス権を得る。業務終了後は速やかに管理者Xに依頼し、アクセス権を抹消する。」の如き記述である。

【0280】

さらに、本実施の形態1では、プロダクトレベルポリシーとして、2レベルの

プロダクトレベルポリシーを作成する。

【0281】

第1レベルは、エグゼクティブレベルポリシーやコーポレートレベルポリシー等と同様に、自然言語で情報セキュリティシステムを構成する各構成装置の設定を記述したものであり、上で述べた例もこの第1レベルのプロダクトレベルポリシーである。

【0282】

第2レベルは、特定商品の特定言語で情報セキュリティシステムを構成する各構成装置の設定を記述したものであり、たとえば、具体的な装置の設定を記述したスクリプトである。すなわち、各機器（ハードウェアだけでなくソフトウェアも含む）の設定スクリプトそのものを記述したものであり、そのまま、各機器の設定に用いることができるものである。本実施の形態1では、プロダクトレベルポリシーとして各装置の具体的なスクリプトを作成しているため、実際にファイアーウォールやルータなどの装置の設定を行う際の労力が軽減できるという効果がある。

【0283】

回答の分析

セキュリティポリシーのドラフトは、質問とその回答により作成されている。このプロセスにおいては、回答にばらつきや矛盾が生じる可能性がある。また、回答が正しいとは限らない。

【0284】

そこで、ステップ2においては、さらに以下のことを実行する。

【0285】

まず、複数の回答に矛盾があるか否か調査する。さらに、セキュリティポリシーのドラフトと、インタビューの回答から想定される情報システムとの比較を行う。そして、セキュリティポリシーのドラフトと、実際の情報システムの実査を行ってプルーフ（検証）を行った情報システムとの比較を行って、その差異を検出する。

【0286】

実際の調査は、エキスパートシステムである分析装置を用いて実行する。この分析装置30の構成ブロック図が図7に示されている。この図に示すように、分析装置30は、回答群に互いに矛盾する回答があるか否か検査する矛盾検査手段32を備えている。この検査結果は、矛盾出力手段40に供給される。

【0287】

矛盾出力手段40は、検査結果を、インタビュー結果矛盾レポートとして外部に出力する。

【0288】

インタビュー結果矛盾レポートの内容は、整合手段41に供給される。整合手段41は、回答間に矛盾があった場合の処理を実行する。この処理は2種類あり、利用者がいずれかを選択することが可能である。

【0289】

- (1) 各メンバーの職務内容に基づいて、知識ベースを利用して、最も確からしい回答を示す。利用者はこの最も確からしい回答を採用することもあるし、自分で正しい回答を決定することもある。

【0290】

- (2) 矛盾点に関し、再インタビューを実施する。又は実際に調査を行って情報システムの実態を知る。再インタビューと実際の調査との双方を実施することも好ましい。

【0291】

このようにして整合をとったインタビューの結果（すなわち回答）は、仮想構築手段34に供給される。

【0292】

仮想構築手段34は、整合がとれた回答群に基づき、その団体の情報システムを仮想的に構築する。さて、このようにして仮想構築手段34が構築した情報システムの構成や運用は差異出力手段38に供給される。

【0293】

また、分析装置30は、その団体の実際の情報システムの構成や運用を入力する実システム入力手段36を備えている。この実システム入力手段36が入力し

た実システムの構成や運用は、上記差異出力手段38に供給される。

【0294】

上述したように、仮想的な情報システムはインタビューによってのみ構築されている。したがって、実システムとは異なっている可能性がある。そのため、実査によって、この仮想的な情報システムを実際の情報システムでプルーフしたものと、セキュリティポリシーのドラフトとの比較をすれば、一層正確に現在の実システムの修正すべき点を知ることができる。

【0295】

このプルーフをするための実査は、精密にすればするほど好ましい。しかし、情報システムのすべてを実査するのは、大きな労力とコストが必要である。さらに、インタビューをした意味が希薄になってしまう。

【0296】

そこで、一般には、インタビューの回答を補助できる程度の実査を行い、上記仮想的情報システムのプルーフをし、プルーフをした情報システムとセキュリティポリシーの差異分析を行うのが、効率的である。

【0297】

たとえば、インタビューの回答に矛盾がある部分を重点的に実査することも好ましい。さらに、被質問者であるメンバーが忘れてしまった等の理由により回答できない部分を重点的に実査することも好ましい。

【0298】

どの程度、実査を行うかは、要求される精度、期限、コストなどによって決定すべきである。このようにして、求めた差異は、分析レポートとして出力される。

【0299】

さらに、差異出力手段38には、セキュリティポリシーのドラフトが供給される。このような構成の下、差異出力手段38は、以下の2つの比較を実行し、それぞれ差異を検出・出力する。

【0300】

(1) セキュリティポリシーのドラフトと、インタビュー結果との差異分析。

【0301】

(2) セキュリティポリシーのドラフトと、インタビュー結果を実査によってプルーフをとったもののとの差異分析。

この(1)の差異分析においては、セキュリティポリシーのドラフトと、仮想構築手段34が構築した情報システムとの比較が実行される。この両者は、基本的には、メンバーへのインタビューの結果(回答)に基づき、構築されているため、ほとんど差はない場合もある。

【0302】

たとえば、インタビューの回答が「パスワードが無制限に有効」となる場合もある。しかし、セキュリティポリシーにおいて、パスワードが無制限に有効とすることはできない。パスワードに期限があることはセキュリティポリシーの基本的な要件であり、これなくしてセキュリティポリシーとは言えない。

【0303】

したがって、セキュリティポリシーのドラフトと、上記インタビュー結果の差異は存在しうる。この検出した差異は、分析レポートとして出力される。

【0304】

この分析レポートによって、インタビューの結果がセキュリティポリシーの観点から修正すべき点を見つけることができる。

【0305】

また(2)の差異分析においては、セキュリティポリシーのドラフトと、上記構築した仮想的な情報システムを実査によってプルーフしたものと、の比較が実行される。

【0306】

なお、これら(1)及び(2)の比較は、いずれか一方のみを行ってもよいし、双方を実行してもかまわない。まず、(1)の比較を実行し、不十分であると判断する場合には、さらに(2)を実行することも好ましい。

【0307】

また、後述するレベル2の実査と分析で得られた優先度を考慮し、優先度の高い部分を実査の対象とすることも好ましい。

【0308】

次に、図5には、本ステップ3の動作を表すフローチャートが示されている。このフローチャートは上記図1のステップS1-2をより詳細に表したものである。

【0309】

ステップS5-5においては、矛盾検査手段32を用いて、回答群中に矛盾のある回答があるか否か検査する。また、ステップS5-6においては、差異出力手段38を用いて、セキュリティポリシーのドラフトと、インタビュー結果との間に差異があるか否か検査する。ここで、インタビュー結果とは、インタビューの回答によって構築した仮想情報システムと、この仮想情報システムを実査によってブルーフしたシステム、の2種類を含む。

【0310】

このように、本実施の形態1によれば、図7に示すような分析装置30を用いているため、回答群に含まれる回答の間に矛盾があるか否か、回答の内容と実システムとの間に差異があるか否か、を迅速に知ることができる。

【0311】

なお、分析装置30は、いわゆるエキスパートシステムであり、上記各手段は、コンピュータ上で動作するソフトウェアで実現することが望ましい。

【0312】

C. ステップ3：システム及びその運用の実査・分析

このステップでは、構築したセキュリティポリシーのドラフトと、実際の情報システム及びその運用手法との差異を検査し、分析を行う。この分析は、差異を見つけだすことに加え、さらに、その対策案を優先度と共に示すために行う。

【0313】

このステップの実査・分析は以下の通りである。

【0314】

このステップ3の実査と分析では、上記ステップS1-2で得た差異を、人的体制の差異、運用方法の差異、技術的対策の差異、の3種類に分類する。そして

、各差異毎に、その対策と優先度を検討する。

【0315】

以下、ネットワークポリシーについて差異がある場合の対策と優先度の例を示す。

【0316】

(1) 差異1

種類 : 人的体制の差異

内容 : ネットワークポリシーでは、ネットワークセグメントの管理者を明らかにする、となっているが、実システムでは明らかではない。

対策 : 管理者又は所有者を明確に割り当てる。

【0317】

優先度 : 即刻

(2) 差異2

種類 : 技術的対策の差異

内容 : ネットワークポリシーでは、ネットワークのユーザ認証で使用するパスワードは長期間使用していなければ抹消されると規定されている。しかし、実システムでは抹消する仕組みがない。

対策 : 30日間使用しないユーザアカウントがあればそのパスワードを抹消する仕組みを設ける。

【0318】

優先度 : 高い

このように、本実施の形態1によれば、回答群と、実システムとの差異を解消するための対策が立てやすくなるため、セキュリティポリシーと実システムとの間の不一致をなくすことが容易となる。

【0319】

D ステップ4 : ポリシー調整・ルール調整

さて、上記ステップ3によって、実システムとセキュリティポリシードラフトとの間の不一致点が明確になり、またそれに対する対策と優先度が明らかになった。本ステップ4では、対策の検討と、実際の作業を実行する。

【0320】

対策は、大きく2種類に分かれる。

【0321】

(1) セキュリティポリシードラフトに調整を加えて実システムに合わせる。

(2) 実システム側の運用ルール等を調整する。

【0322】

以下、これらを詳細に説明する。

【0323】

D-1 セキュリティポリシードラフトの調整

セキュリティポリシーのドラフトは、既に説明したようにグローバルガイドラインと呼ばれる、標準的なセキュリティポリシーを構築するための基本的な項目、内容を、適宜組み合わせで構築している。現在、有名なグローバルガイドラインは数種類知られており、本実施の形態1では、その数種の中から適宜ルールや方針等を取り出して組み合わせでセキュリティポリシーの構築を行っている。ドラフトの段階では、これら数種のグローバルガイドライン中最も条件の厳しいものを選び出し、セキュリティポリシーのドラフトに組み込んでいる。

【0324】

換言すれば、これらグローバルガイドラインは、その種類によって各規定の強度が異なっているのである。たとえば、あるグローバルガイドラインでは、パスワードの有効期限を60日としているが、他のグローバルガイドラインではこれを180日と規定している。

【0325】

すなわち、ドラフトの段階では、最も厳しい条件で各ルール等が構築されているのである。したがって、団体側の意向によっては、セキュリティポリシーのドラフト内の各ルールの強度が強すぎると判断される場合もあろう。このような場合には、適宜弱いルールに変更することが好ましい。

【0326】

たとえば、同一のパスワードの有効期限を60日とするルールが厳しい、すな

わち強いルールである場合には、団体側との話し合いによって有効期限を180日に変更する、すなわち弱いルールに変更するのである。

【0327】

このように、各団体の意向と強度のバランスの判断から、ルールの強度を変更すれば、実システムと合致したセキュリティポリシーを構築することが可能である。

【0328】

このようにして、セキュリティポリシーのドラフトの調整が実行される。

【0329】

D-2 ルール調整

上述したレベル2の実査と分析において説明した対策に基づき、実システム側の運用を調整する。このルール調整は、運用方法を変更するものや、さらに、セキュリティシステム（たとえばファイアーウォール）のルール設定の修正等がある。

【0330】

E ステップ5：プライオリティプランニング

上記ステップ4までで、団体の実際の情報システムに関するセキュリティポリシーの構築が完了する。

【0331】

しかし、今後、このセキュリティポリシーに合わせてセキュリティ対策を順次実行していく必要がある。そこで、本ステップ5では、優先順位を含めて各種対策を検討し、リストにしておく。このようなリストを作成しておくことで、今後のセキュリティ対策の計画を立てることができる。さらには、その計画に基づき、予算の検討を行うことができる。すなわち、情報セキュリティ対策の予算化を実現することができるのである。このようなリストがなければ、将来の情報セキュリティ費用がどの程度かかるのか見通しが立たず、予算化が困難になることも考えられる。

【0332】

セキュリティ対策には、セキュリティシステムの導入及びテストの他に、セキ

セキュリティポリシーを遵守するための従業員の教育、システムログの分析、等の作業も含まれる。

【0333】

また、セキュリティポリシーには、ネットワーク監視と、セキュリティポリシーに基づく運用の監査と、セキュリティポリシーの見直しと、が含まれる。

【0334】

なお、団体側の情報システムの変更、運用の変更等に合わせて、セキュリティポリシーも変更をする必要がある。そこで、定期的にセキュリティポリシーの見直しを行う必要がある。

【0335】

F ステップ6：セキュリティ強化策実行

上記ステップ5において作成した優先順位を含めたセキュリティ対策リストに基づき、実際にセキュリティ強化策を実行していく。この実行は上記リスト及びセキュリティポリシーに従ったものであり、円滑に作業を進めることが可能である。

【0336】

以上述べたように、本実施の形態1では、セキュリティポリシーの構築からメンテナンスまでを6ステップに分けて実行している。したがって、セキュリティポリシーを段階的に構築、実行していくことが可能であり、団体側の要望に合った作業の進め方を実現可能である。

【0337】

実施の形態2（業種の考慮）

上記実施の形態1においては、団体のメンバーの職務内容によって質問が変更される例を説明したが、特に、その団体の業種は考慮していない。

【0338】

しかし、たとえば金融業と製造業とでは、構築するセキュリティポリシーも異なるべきである。

【0339】

そこで、本実施の形態2では、団体の業種を考慮したセキュリティポリシーを

構築することを提案する。以下、団体の業種を考慮したセキュリティポリシー（のドラフト）を構築するための種々の工夫を説明する。

【 0 3 4 0 】

上記図 4 のセキュリティポリシードラフト構築装置 2 0 においては、メンバーの職務内容によって質問が変更される旨説明した。本実施の形態 2 ではこれに加えて、その団体の業種によって質問を変更する例を説明する。

【 0 3 4 1 】

図 9 には、本実施の形態 2 のセキュリティポリシードラフト構築装置 1 2 0 の構成ブロック図が示されている。

【 0 3 4 2 】

セキュリティポリシードラフト構築装置 1 2 0 は、図 4 に示したセキュリティポリシードラフト構築装置 2 0 とほぼ同様の構成である。

【 0 3 4 3 】

異なる点の 1 つは、セキュリティポリシードラフト構築装置 1 2 0 が、インタビューを受けるメンバーが属する団体の業種に基づいて質問を生成する質問生成手段 1 2 2 を備えていることである。この質問生成手段 1 2 2 は、メンバーの職務内容だけでなく、団体の業種に基づいて質問を生成するのである。

【 0 3 4 4 】

また、記憶手段 1 2 4 には、業種によって異なる質問があらかじめ格納されている。質問生成手段 1 2 2 は、入力された業種に基づき、その業種に対応する質問群を記憶手段 1 2 4 から読み出すのである。

【 0 3 4 5 】

回答保管手段 1 2 6 は、図 4 における回答保管手段 2 6 とほぼ同様の動作を実行する。

【 0 3 4 6 】

このような構成によって、各業種に対応した質問を生成し、よりきめの細かいセキュリティポリシーを構築可能である。

【 0 3 4 7 】

たとえば、金融業の団体に対しては、「預金者リストの管理はどのようにして

いるか？」等の質問を生成すべきであるが、製造業の団体に対してそのような質問を生成する意味はない。逆に、製造業の団体に対して「製造ロット毎の進捗データの管理はどのようにしているか？」等の質問を生成すべきであるが、金融業の団体に対してそのような質問を生成する意味はない。

【0348】

したがって、本実施の形態2によれば、団体の業種によって質問を変更し、より詳細な内容についての質問を行うことができ、団体の情報システムの細部（運用・管理も含む）をよりよく知ることが可能である。

【0349】

なお、ここで言う質問の変更とは、上述した職務内容と同様に、質問のコースが変更されることを意味する。すなわち、金融業の団体に対しては、金融業向けの質問群を含むコースが適用され、製造業の団体に対しては、製造業向けの質問群を含むコースが適用されるのである。各コースでは、そこに含まれる質問に対する回答の内容によって次の質問が変更されることは実施の形態1と同様である。

【0350】

さて、図9のドラフト構築手段128は、基本的には図4におけるドラフト構築手段28と同様のものである。ただし、図9のドラフト構築手段128の質問生成手段122が生成した、より詳細な内容の質問に対する回答に基づいてセキュリティポリシーのドラフトを構築しているため、既に述べたように、より精密なセキュリティポリシーのドラフトを構築可能である。

【0351】

本実施の形態2におけるセキュリティポリシーのドラフトの構築動作は、上記図5におけるフローチャートとほぼ同様である。

【0352】

異なる点は、ステップS5-1において、その団体の業種が、メンバーの職務内容と同様に質問生成手段122に供給される点である。この結果、質問生成手段122は、メンバーの職務内容と、団体の業種に基づき適切な質問を生成することが可能である。

【 0 3 5 3 】

このように、本実施の形態 2 においては、団体の業種を考慮した質問を生成しているため、インタビューによって団体の情報セキュリティシステムをより詳しく知ることができる。その結果、より精密なセキュリティポリシーの構築を行うことが可能である。

【 0 3 5 4 】

なお、上記説明では、団体の業種に基づき質問を変更する例を示したが、団体の規模によって変更することも好ましい。

【 0 3 5 5 】

また、上記説明では、質問の変更の例として質問のコースの変更を示したが、その他種々の変更の方式を採用することができる。たとえば、基本的な質問文の枠組みを定めておき、その文の中の用語を、業種に合わせて変更することも好ましい。具体的には、一般企業に対する質問の文中では「社長」の言葉を用いているが、銀行の場合にはこの「社長」を「頭取」の言葉に置き換える如き変更の方式が考えられる。

【 0 3 5 6 】

実施の形態 3（特定の業種の勧告や規定の考慮）

実施の形態 1 で述べた例においてはグローバルガイドラインに基づき、セキュリティポリシーを構築している（ステップ S 5 - 4）。このグローバルガイドラインは、ある特定の目的をもって作成される場合も多いが、概ね汎用的に利用可能なように構成されている。

【 0 3 5 7 】

この汎用的なグローバルガイドラインに対して、特定の業種の種々の勧告や規定が知られている。これらの勧告や規定は、グローバルガイドラインと異なり、特定の業種向けの勧告や規定であることが明確に謳われているものである。これらの勧告や規定も情報セキュリティに言及している場合が多いため、グローバルガイドラインと同様にセキュリティポリシーの構築の際に利用することが望ましい。

【 0 3 5 8 】

たとえば、日本の金融情報システムセンター（FISC：The Center for Financial Industry Information Systems）では、セキュリティ対策のための安全対策基準の策定や、セキュリティポリシーの普及を行っている。そして、このFISCは、「金融機関等コンピュータシステムの安全対策基準」等の刊行物を発行している。

【0359】

本実施の形態3では、金融業に対してセキュリティポリシーを構築する場合には、グローバルガイドラインだけでなく、この「金融機関等コンピュータシステムの安全対策基準」にも基づいて、セキュリティポリシーを構築することを提案する。この結果、特定の業種においては、その業種に的を絞った勧告や規定に基づきセキュリティポリシーが構築されるため、より緻密なセキュリティポリシーが構築可能である。

【0360】

このように、特定の業種向けの勧告や規定をグローバルガイドラインと同様に利用するセキュリティポリシードラフト構築装置の構成が図9に示されている。

【0361】

この図に示すように、セキュリティポリシードラフト構築装置220の構成は、図8のセキュリティポリシードラフト構築装置120とほぼ同様である。異なっている点は、団体の業種に関する情報が、質問生成手段222だけでなく、ドラフト構築手段228にも供給されている点である。そして、ドラフト構築手段228は、団体の業種に基づき、セキュリティポリシーのドラフトの構築に用いるべき特定の勧告や規定を利用者に示し、利用者はこれを選択することが可能である。なお、選択される特定の勧告や規定は、1個には限られず、2個以上とする場合もある。もちろん、利用者は、示される特定の勧告や規定を無視し、一般的なグローバルガイドラインを選ぶことも可能である。

【0362】

また、以下の点が本実施の形態3において特徴的な事項である。

【0363】

第1に、ドラフト構築手段228が、団体の業種に基づき、利用する特定の業

種向けの勧告や規定を選択することが本実施の形態3において新規な事項である。このような動作を行うことによって、たとえば金融業においては、金融業向けの勧告や規定を利用したセキュリティポリシー（のドラフト）を構築することが可能である。

【0364】

第2に、記憶手段224内に特定の業務向けの勧告や規定に関する情報が、グローバルガイドラインに関する情報と同様に格納されていることである。この情報が格納されていることによって、質問生成手段222はその団体の業種向けに制定されている勧告や規定に則した質問を生成することができる。また、この格納されている情報に従って、ドラフト構築手段228は、その団体の業種向けに制定されている勧告や規定に基づいたセキュリティポリシーを構築することが可能である。

【0365】

また、本実施の形態3におけるセキュリティポリシーの構築動作は、基本的に図5のフローチャートとほぼ同様である。異なる点は以下の通りである。

【0366】

第1に、ステップS5-1において、その団体の業種が質問生成手段222に供給され、その団体の業種向けの勧告や規定が示される。利用者が示された勧告や規定を選択すれば、この勧告や規定に則した質問が生成される点が第1に異なる点である。そのような勧告や規定が存在しない場合には、実施の形態1～実施の形態3と同様にしてグローバルガイドラインに基づいて質問が生成される。

【0367】

第2に、ステップS5-4において、その団体の業種がドラフト構築手段228にも供給され、ドラフト構築手段228が、その団体の業種向けの勧告や規定に則してセキュリティポリシーのドラフトを構築する点である。この動作も、利用者がその勧告や規定を選択した場合の動作である。そのような勧告や規定が存在しない場合には、実施の形態1～実施の形態2と同様にしてグローバルガイドラインに基づいてセキュリティポリシーのドラフトが構築される。

【0368】

たとえば、グローバルガイドラインによれば、「基幹ネットワークの責任者を立てていますか？」という質問が生成される。しかし、特に金融業の場合には、上記「金融機関等コンピュータシステムの安全対策基準」に基づき、「ATM（Automatic Teller Machine：現金自動預入支払機）ネットワークの責任者を立てていますか？」という質問が生成される。

【0369】

このような質問は、上記実施の形態2で述べた「業種によって質問を変更する」手法で生成すればよい。たとえば、業種が金融業である場合には、上記「金融機関等コンピュータシステムの安全対策基準」に則した質問が生成され、インタビューに用いられるのである。このような質問を生成するエキスパートシステムは、上記「金融機関等コンピュータシステムの安全対策基準」に関する情報を含む知識ベースを利用することによって構成することができる。

【0370】

このような手法でセキュリティポリシーを構築することによって、より緻密なセキュリティポリシーを構築可能である。

【0371】

項目の重複

グローバルガイドラインには存在せず、上記特定の業種の勧告や規定にのみ存在する項目は、もちろん上記特定の業種の勧告や規定に基づきセキュリティポリシーが構築される。

【0372】

逆に、グローバルガイドラインにのみ存在し、上記特定の業種の勧告や規定には存在しない項目は、上記実施の形態1と同様にグローバルガイドラインに基づきセキュリティポリシーが構築される。

【0373】

さらに、グローバルガイドラインにも存在し、かつ、上記特定の業種の勧告や規定にも存在する項目は、上記特定の業種の勧告や規定に基づきセキュリティポリシーを構築することが好ましい。

【0374】

実施の形態 4（利用者によるグローバルガイドラインの指定）

これまで、グローバルガイドラインや、特定の業種の勧告や規定に基づくセキュリティポリシーの構築を説明した。

【 0 3 7 5 】

しかし、利用者が、ある特定のグローバルガイドラインに基づいたセキュリティポリシーを構築したいと望む場合も考えられる。たとえば、ある所定の国（たとえば米国）においては、グローバルガイドラインとして特定のグローバルガイドライン（たとえば C o b i t）がデファクトスタンダードとして利用されている場合がある（C o b i t に関しては後に説明する）。このような状況下では、セキュリティポリシーもこの特定のグローバルガイドライン（たとえば C o b i t）に基づき構築することが望ましい場合も多い。

【 0 3 7 6 】

そこで、本実施の形態 4 では、セキュリティポリシーの構築に際して利用するグローバルガイドライン等を、利用者が明示的に指定可能に構成することを提案する。

【 0 3 7 7 】

本実施の形態 4 のセキュリティポリシードラフト構築装置 3 2 0 の構成ブロック図が図 1 0 に示されている。この図に示すように、利用者が指示するグローバルガイドラインに関する情報は、質問生成手段 3 2 2 とドラフト構築手段 3 2 8 とに供給される。

【 0 3 7 8 】

質問生成手段 3 2 2 は、実施の形態 1 と同様に、メンバーの職務内容に基づいて質問（群）を生成する。本実施の形態 5 においては、質問生成手段 3 2 2 は、質問生成の際に、利用者が指示するグローバルガイドラインに則した質問を生成する。なお、利用者は、1 個だけでなく複数個のグローバルガイドラインを指示可能である。

【 0 3 7 9 】

ドラフト構築手段 3 2 8 は、利用者が指示したグローバルガイドラインに基づきセキュリティポリシーのドラフトを構築する。

【 0 3 8 0 】

本実施の形態 5 のセキュリティポリシーのドラフト構築の動作は、上記図 5 に示した動作と、以下の点を除きほぼ同様である。

【 0 3 8 1 】

第 1 に異なる点は、ステップ S 5 - 1 において、利用者が指示するグローバルガイドラインに則した質問の生成が行われる点である。

【 0 3 8 2 】

第 2 に異なる点は、ステップ S 5 - 4 において、利用者が指示するグローバルガイドラインに則したセキュリティポリシーのドラフトの構築が行われる点である。

【 0 3 8 3 】

このように本実施の形態 5 によれば、セキュリティポリシーを構築する際に利用するグローバルガイドライン等を選択することができる。そして、利用者が選択したグローバルガイドラインに則して質問が生成され、その答えに基づいてセキュリティポリシーのドラフトが構築される。その結果、利用者が所望するグローバルガイドラインに則したセキュリティポリシーを構築することが可能である。

【 0 3 8 4 】

たとえば、利用者が後述する B S 7 7 9 9 を選択した場合には、B S 7 7 9 9 に適合するため（又はさせるため）のセキュリティポリシーを構築することが可能である。

【 0 3 8 5 】

グローバルガイドライン

グローバルガイドラインとして、広く知られているものの例を以下に示す。

【 0 3 8 6 】

(1) B S 7 7 9 9

B S 7 7 9 9 は、1 9 9 5 年に、B S I (British Standards Institution : 英国規格協会) によって制定された。この B S 7 7 9 9 は、情報セキュリティにおけるベストプラクティス（最適慣行）をまとめた基本的な管理項目（コントロー

ル)を規定する。

【0387】

このBS7799の規格は、産業界はもとより行政、あるいはNGO(Non Governmental Organization: 非政府組織)、NPO(Non Profit Organization: 非営利の民間組織)において、またその組織規模を問わず情報資産を保護する必要がある場合、情報セキュリティの範囲を明確にする際の一つの規範・基準として使用されることを目的としている。

【0388】

したがって、後述するISO/IEC13335「ITセキュリティマネジメントガイドライン(GMITS)」や、ISO/IEC15408「ITセキュリティ評価基準」などと同様の目的を持った規格である。このBS7799がこれら他のグローバルガイドラインと異なる特徴的な点は、次の2点である。

【0389】

第一に、他の規格がITを対象としてセキュリティ技術の詳細まで規定しているのに対して、BS7799はマネジメントシステムに対する普遍的、包括的なガイド、基準を示していることである。第二に、電子媒体に限定せず紙媒体など様々な情報資産をセキュリティの対象としていることである。

【0390】

近年、このBS7799は国際的に非常に注目されている。この理由は、情報セキュリティの詳細な個別コントロールはもちろん重要であるが、ISO9000等システム規格の要求事項にみられるような、(リスク分析に基づき)マネジメントプランを立案し、必要な資源配分及び運用を監視し、客観的に見直すという仕組みが、情報セキュリティマネジメントにも有効であるとの認識が広まったことによるものと言われている。

【0391】

BS7799は、第1部:情報セキュリティ管理実施基準及び、第2部:情報セキュリティシステム仕様の2つの部で構成されている。第1部ではベストプラクティスを示し、マネジメントへのアドバイスを与えるガイドラインが示されて

いる。また、第2部は、マネジメントの枠組みを開発すること及び「システム監査」の基準が示されている。この第1部（BS 7799-1）が、ISO 17799としてISO化される。

【0392】

(2) GASSP

GASSP (Generally Accepted System Security Principles) は、Good Practiceの促進と、リスクの軽減と、リスクの影響の軽減と、を目的とする。GASSPは、OECDの情報セキュリティ方針を使用して、階層モデル化し、方針を詳細にわたって展開している。

【0393】

最上位の基本となる方針は、Pervasive Principlesと呼ばれ、セキュリティの目標概念を掲示している。

【0394】

次の階層の方針は、Broad Function Principlesと呼ばれ、Pervasive Principlesの具体的な実行について既述している。

【0395】

さらに下の階層の方針は、Detailed Principlesと呼ばれ、環境に応じた詳細なセキュリティガイドラインが記述されている。

【0396】

これらの方針は、管理や製品関連のガイドラインだけでなく、個人や組織のプライバシーの管理についても記述している。

【0397】

(3) GMITS

GMITS (The Guidelines for the management of IT Security) は、ISO (International Organization for Standardization) によって作成されている。このGMITSは、情報技術のセキュリティに関連した運用管理、計画を対象とした標準を設定することを目的としている。

【0398】

GMITSは、5部から構成されている。

【0399】

Part1: Concepts and models for IT Security

このPart1では、情報セキュリティの概要を記述している。

【0400】

Part2: Managing and Planning IT Security

このPart2では、セキュリティライフサイクルと同様の作業について記述している。

【0401】

Part3: Techniques for the management of IT Security

このPart3では、Part2に関し、その詳細を記述している。

【0402】

part 4: Selection of Safeguards

このpart4では、セキュリティ要件に従ってどのような対応策を選択するのかについて記述している。

【0403】

part 5: Management Guidance on Network Security

このpart5は、現在、ドラフト版である。

【0404】

ネットワークセキュリティ上の管理に関する作業について記述する。

【0405】

(4) ISO/IEC 15408

ISO/IEC 15408は、情報技術を用いた製品やシステムが備えるべきセキュリティ機能に関する要件（機能要件）や、設計から製品化に至る過程でセキュリティ機能が確実に実現されていることの確認を求める要件（保証要件）が集大成された「要件集」である。

【0406】

(5) C o b i t

C o b i t (Control Objectives for information and related Technology) は、複数の分野にまたがるプロセスのフレームワークに適するセキュリティの

規範 (good practice) を示し、管理可能な論理的ストラクチャーを提示する。
このgood practiceは、多くの専門家によって得られた同意をもとに作成されている。そして、このC o b i t は、業務上のリスクや制御の必要性和技術的問題との間にあるギャップの解消に役立つように設計されているグローバルガイドラインである。

【0407】

(6) E U 指令

ここで言うE U 指令は、正式には「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」である。このE U 指令は、個人データの処理の合法性に関する一般規則が規定されており、データの質に関する原則や、データ処理の適法性の根拠に関する原則や、データの対象者に与えられる情報、データの対象者のデータに対するアクセス権等が、規定されている。

【0408】

実施の形態5 (強度の指定)

これまでの実施の形態では、セキュリティポリシーの強度の調整は、図1のステップS 1 - 4 において人為的に行われているのみである。

【0409】

しかし、所望のセキュリティポリシーの強度があらかじめ判明している場合には、ステップS 1 - 2 におけるドラフトの構築段階からその所望の強度を反映させる方が望ましい。

【0410】

また、図1のステップS 1 - 4 においては、各ルールの強度を人為的に調整していた。しかし、強度の指標を定義し、利用者がその指標を用いてセキュリティポリシーの強度を指定し、指定した強度に基づき自動的に各ルールの強度の調整ができれば便利である。

【0411】

本実施の形態5において特徴的なことは、図1のステップS 1 - 2 やステップS 1 - 4 においてセキュリティポリシーの強度を利用者が客観的に指定可能に構

成していることである。

【0412】

このようなことを実現するために、本実施の形態6では、セキュリティポリシーの強度を表す指標を以下のように5種定義している。以下の並びは、強度の強い順である。すなわち、最も強度が強いのが「最高レベル」であり、最も弱いのが「教育機関レベル」である。

【0413】

(1) 最高レベル：政府や軍事組織で必要と考えられるセキュリティ強度を表す。

【0414】

(2) 金融レベル：金融機関に必要と考えられるセキュリティ強度を表す。

(3) 国際レベル：国際的な企業に必要と考えられるセキュリティ強度を表す。

(4) 一般レベル：国内企業に必要と考えられるセキュリティ強度を表す。

(5) 教育機関レベル：教育機関に必要と考えられるセキュリティ強度を表す。

【0415】

ここでは5段階の例を示したが、もちろん強、中、弱の3段階としてもよい。

【0416】

5-A 強度を指定したセキュリティポリシーの構築

ステップS1-2（図1）におけるセキュリティポリシーの強度指標の利用について説明する。利用者は、ステップS1-2（図1）におけるセキュリティポリシーのドラフトを構築する際に、所望の強度を上記5種から選択してドラフト構築装置20に指示する。

【0417】

この指標に基づき、利用者が所望する強度の規定をグローバルガイドラインから取り出すことによって、利用者の望む強度のセキュリティポリシーのドラフトを構築することが可能である。グローバルガイドラインの中には、セキュリティポリシーの強度を表す指標が含まれているものも多いので、このようなことが可

能である。

【0418】

取り出しの動作は、知識ベースの中に各グローバルガイドラインの強度に関する知識を組み込んでおき、この知識ベースを利用して利用者が指示した指標に基づき適切な規定をグローバルガイドラインから取り出すことによって実行される。各グローバルガイドラインの強度に関する知識とは、たとえば、上記5種の強度指標と、この強度指標に対応する規定と、を関連づけた知識である。このような知識を用いることによって、与えられた強度の指標に対応する規定をグローバルガイドライン中から選び出すことが可能である。

【0419】

本実施の形態5のセキュリティポリシードラフト構築装置420の構成ブロック図が図12に示されている。この図に示すように、セキュリティポリシードラフト構築装置420においては、利用者が指示する強度の指標がドラフト構築手段428に与えられる。

【0420】

ドラフト構築手段428は、利用者が指示した強度指標に基づきセキュリティポリシーのドラフトを構築する。この構築動作は、上述したように、指示された強度指標に基づき、指示された強度指標に合致する方針に関する知識を知識ベースの中に組み入れておき、この知識ベースに基づいて、強度指標に合致した方針をグローバルガイドラインから取り出してくることによって実行される。

【0421】

この動作は、要するにある強度指標に対してどのような方針を設定するかに関してあらかじめルールを（知識ベースの中で）取り決めておこうとするものである。

【0422】

また、本実施の形態5におけるセキュリティポリシーの構築動作は、以下の点を除き、基本的に図5のフローチャートとほぼ同様である。

【0423】

第1に異なる点は、ステップS5-1において、質問生成手段422が利用者

が指示した強度に基づき、質問を生成する点である。「強度」は、他のパラメータ（業種等）に比べれば質問に対する影響は少ないが、一般的に強度を強くすれば、より細かい事項に関する質問も生成される。また、一般的に強度を弱くすれば、細かい事項に関する質問が新たに生成される。

【0424】

たとえば、一度セキュリティポリシーを構築した後で、セキュリティポリシーの強度をより強く設定し直すことが考えられる。この場合、利用者が指示するより強い強度指標は、質問生成手段422にも供給されているので、質問生成手段422は、より細かい事項に関する質問を生成する。その結果、団体のメンバー（被質問者）に対する質問をもう一度実施する必要性が一部に生じる場合もある。

【0425】

一方、セキュリティポリシーの強度をより弱く設定し直した場合には、一般的には、新たな質問が生成される可能性はない。したがって、この場合は、質問をもう一度実施することなく、すぐに新たなセキュリティポリシーの構築を行うことが可能である。

【0426】

次に、第2に異なる点は、ステップS5-4において、利用者が指示した強度指標がドラフト構築手段428にも供給され、ドラフト構築手段428が、その強度指標に基づいてセキュリティポリシーのドラフトを構築する点である。

【0427】

この2点以外の動作は図5のフローチャートとほぼ同様である。

【0428】

5-B 強度を指定したセキュリティポリシーの調整

本実施の形態5では、ステップS1-4（図1）におけるセキュリティポリシーの調整も自動的に実行される。図12には、そのようなセキュリティポリシーの調整を実行するセキュリティポリシー強度調整装置500の構成ブロック図が示されている。この図に示すように、セキュリティポリシー強度調整装置500は、強度検査手段502と、強度調整手段504と、記憶手段506と、合成手

段 5 0 8 と、を備えている。

【 0 4 2 9 】

強度検査手段 5 0 2 には、ステップ S 1 - 3 (図 1) までの動作で構築されたセキュリティポリシーのドラフトが供給される。この強度検査手段 5 0 2 は、利用者が指示する強度の指標に基づき、セキュリティポリシーのドラフト内の各ルールが、利用者が指示する強度に合致しているか否か検査する。検査の結果、各ルールが合致していればそのルールはそのまま出力される。一方、合致していない場合はそのルールは強度調整手段 5 0 4 に供給される。強度調整手段 5 0 4 は、供給されてきたルールを、利用者が指示する強度指標に基づき、書き換えて出力する。合成手段 5 0 8 は、強度指標に合致していたルールと、強度指標に合致するように書き換えられたルールと、を合成し、外部に出力する。記憶手段 5 0 6 には、グローバルガイドラインと、グローバルガイドライン中の各ルールと強度指標との対応付けに関する情報と、が記憶されている。

【 0 4 3 0 】

セキュリティポリシー強度調整装置 5 0 0 の動作を表すフローチャートが図 1 3 に示されている。

【 0 4 3 1 】

まず、ステップ S 1 3 - 1 において、セキュリティポリシーのドラフトが強度検査手段 5 0 2 に供給される。

【 0 4 3 2 】

ステップ S 1 3 - 2 においては、強度検査手段 5 0 2 は、供給されたセキュリティポリシーのドラフト中の各ルールが、利用者が指示する強度の指標に合致するか否かを検査する。そして、合致している場合には、後述するステップ S 1 3 - 3 に移行する。一方、合致していない場合には、ステップ S 1 3 - 4 に移行する。

【 0 4 3 3 】

ステップ S 1 3 - 4 においては、ルールを、利用者が指示する強度の指標に合致するように変更する。この変更は、記憶手段 5 0 6 内部のグローバルガイドライン中の各ルールと強度指標との対応付けに関する情報を利用して、強度調整手

段 5 0 4 が実行する。この情報は、グローバルガイドライン中の各ルールが対応する強度指標に関する情報であるため、この情報を利用すれば利用者が指示した強度指標に合致したルールを知ることが可能である。そしてこのようにして知ったルールを、同じく記憶手段 5 0 6 内部のグローバルガイドラインから取り出し、強度指標と合致しないルールを、この取り出した合致するルールと置き換えるのである。

【 0 4 3 4 】

ステップ S 1 3 - 3 においては、強度指標に合致していたルールと、変更したルールと、が合成されて出力される。この合成出力動作は、合成手段 5 0 8 によって実行される。

【 0 4 3 5 】

このようにして、セキュリティポリシーのドラフト内の各ルールを、利用者が指示する強度の指標に合致させることができる。

【 0 4 3 6 】

なお、本実施の形態 5 における強度検査手段 5 0 2、強度調整手段 5 0 4、合成手段 5 0 8 は、コンピュータ上で動作するソフトウェアで構成することが好ましい。また、記憶手段 5 0 6 は、ハードディスク、CD-ROM、DVD等の種々の記憶媒体で構成することが望ましい。

【 0 4 3 7 】

ルールと強度指標の関係

ステップ S 1 3 - 2 におけるルールの強度と、利用者が指示する強度指標で表される強度とが合致しない場合についてより詳細に説明する。

【 0 4 3 8 】

ルールが強度指標で示される強度より弱い強度のルールである場合には、そのルールは強度指標に合致していないと判断され、より強い強度のルールと置き換えられる。

【 0 4 3 9 】

たとえば、ルールが教育機関レベルであり、利用者が指示した強度が金融レベルである場合には、そのルールは金融機関レベルのルールに置き換えられるので

ある。また、たとえば、パスワードの有効期間が120日から30日に短縮され、より厳しい（強い）レベルのルールに置き換えられるのである。

【0440】

そして、ルールが強度指標で示される強度より強い強度のルールである場合には、そのルールは強度指標に合致していないと判断され、より弱い強度のルールと置き換えられる。

【0441】

たとえば、ルールが最高レベルであり、利用者が指示した強度が一般レベルである場合には、そのルールは一般レベルのルールに置き換えられるのである。また、たとえば、パスワードの保存期間が、最高レベルでは1週間であるが、それでは厳しすぎる場合、利用者は一般レベルを指定する。すると、たとえばパスワードの有効期間が100日に延長され、より緩い（弱い）レベルのルールに置き換えられるのである。

【0442】

実施の形態6（構築範囲の選択）

これまで述べた例においては、セキュリティポリシーはその団体の全体に対して作成されている。しかしながら、その団体の一部のシステムに対してのみセキュリティポリシーを構築したいという要望も多いと考えられる。

【0443】

そこで、利用者がセキュリティポリシーを構築する範囲を指定し、この範囲に基づいてセキュリティポリシーを構築する装置・方法を採用すれば、利用者がセキュリティポリシーを構築したいと考える部分に対してのみセキュリティポリシーを構築することができ便利である。

【0444】

図14には、このようなセキュリティポリシードラフト構築装置520の構成を表す構成ブロック図が示されている。この図に示すセキュリティポリシードラフト構築装置520の構成は、図10や図11で説明したセキュリティポリシー構築装置320や420と同様である。

【0445】

異なる点は、以下の2点である。

【0446】

・ドラフト構築手段528に利用者が指示するセキュリティポリシーの構築範囲が供給されている点。

【0447】

・質問生成手段522に利用者が指示するセキュリティポリシーの構築範囲が供給されている点。

【0448】

このような構成によって、ドラフト構築手段528は、利用者が指示する範囲に関するセキュリティポリシーを構築するので、利用者は必要な範囲のセキュリティポリシーを効率的に得ることが可能となる。

【0449】

また、質問生成手段522も利用者が指示する範囲に関する質問のみを生成するので、無駄な質問がなくなり、効率的な質問を行うことができる。ただし、質問生成手段522には、必ずしも利用者が指示する範囲が供給されなくてもよい。質問が多くてもセキュリティポリシーの構築には影響がないからである。また、利用者が指示した範囲と関係ない質問の場合にはインタビュー時に、質問者が質問をスキップすることもできる。したがって、利用者が指示した範囲が質問生成手段に522に供給されていることは必須の要件というわけではない。

【0450】

さて、利用者は、セキュリティポリシーの構築範囲を種々の手法で指示することができる。

【0451】

(1) まず、利用者はセキュリティポリシーの構築範囲をプロダクト（製品）のレベルで指示することができる。たとえば、利用者は「VPN」に関するセキュリティポリシーのみを構築したい場合は、この「VPN」を指示することにより、VPNに関するセキュリティポリシーを構築させることができる。また、WEB、Eメール、ファイアーウォール、等の具体的なハードウェアやソフトウェア、もしくは機能を指示することによって、利用者はその具体的なハードウェア

やソフトウェアに関するセキュリティポリシーの構築を指示することができる。

【0452】

(2) 次に、利用者は、使用目的によってセキュリティポリシーの構築範囲を指示することができる。たとえば、利用者は「外部委託」に関するセキュリティポリシーのみを構築したい場合は、この「外部委託」を指示することにより、外部委託を実行する部分に関してセキュリティポリシーを構築させることができる。また、電子商取引（Eコマース）、データセンター、等の具体的な使用目的、もしくは用途を指示することによって、利用者はその使用目的や用途に関する範囲のセキュリティポリシーの構築を指示することができる。

【0453】

(3) さらに、利用者は、団体の組織としての観点からセキュリティポリシーの構築範囲を指示することができる。たとえば、利用者は「本社」に関するセキュリティポリシーのみを構築したい場合は、この「本社」を指示することにより、本社に関するセキュリティポリシーを構築させることができる。また、支店を指示することによって、支店のセキュリティポリシーを構築させることができる。さらに、利用者は、ネットワークや、ホスト等を指示することによって、ネットワークに関するセキュリティポリシー、ホストに関するセキュリティポリシーをそれぞれ構築させることができる。

【0454】

本実施の形態7のセキュリティポリシー構築の動作は、上記図5に示した動作とほぼ同様である。異なる点は以下の通りである。

【0455】

・第1に、図5におけるステップS5-4において、利用者が指示する範囲に基づき、セキュリティポリシーのドラフトの構築が行われる点である。

【0456】

・第2に、図5におけるステップS5-1において、利用者が指示する範囲に関する質問のみが生成される点である。

【0457】

この第2の相違点は、必ずしも必須の要件ではない。既に説明したように、質

間が、利用者が指示した範囲外のものであっても、セキュリティポリシーの構築には直接には支障がないからである。また、質問者が適宜そのような質問をスキップすることも考えられるので、質問自体は、実施の形態1などと同様でもかまわない。

【0458】

このセキュリティポリシーのドラフトの構築は、図14のドラフト構築手段528が実行する。このようなことを実現するために、記憶手段524中には、グローバルガイドライン中の各ルールが、どの範囲にあるかについての知識ベースが構築されている。すなわち、各ルールが、「本社」の範囲にあるのか、それとも「支店」の範囲にあるのか、等の知識ベースが記憶手段524中に格納されている。この知識ベースを参照することによって、ドラフト構築手段528は、利用者が指示した範囲に含まれるルールのみを用いてセキュリティポリシー（のドラフト）を構築する。

【0459】

このようにして、本実施の形態7によれば、利用者が指示した構築範囲に基づき、その範囲のセキュリティポリシー（のドラフト）の構築を行うことができる。

【0460】

なお、本実施の形態6では、実施の形態1と同様に質問生成手段522がメンバー（被質問者）の職務内容に応じて質問を生成する例を示したが（図14）、質問生成手段が職務内容に関わらず一般的な質問をメンバーに対して行う構成としてもよい。

【0461】

実施の形態7（プログラム及び記録媒体）

これまで述べた各実施の形態における各手段は、実際には、プログラム及びそのプログラムを実行するプロセッサから構成することが好適である。

【0462】

図15には、コンピュータと各種のプログラムが格納されたハードディスク装置600を備えたコンピュータ602が示されている。

【0463】

このハードディスク600中には、上述した各実施の形態1～7で説明した質問生成手段12や、回答保管手段16、ドラフト構築手段18等の各手段の動作を実行するプログラムが格納されている。コンピュータ602のプロセッサがこれらのプログラムを実行することによって、このコンピュータ602は、質問生成手段や、回答保管手段、ドラフト構築手段等に相当する動作を実行可能である。

【0464】

また、図7における矛盾検査手段32や、矛盾出力手段40、整合手段41、仮想構築手段34、差異出力手段38、実システム入力手段36等の動作を実行するプログラムもハードディスク600中に格納されている。コンピュータ602のプロセッサがこれらのプログラムを実行することによって、このコンピュータ602は、矛盾検査手段32等の動作を実行可能である。

【0465】

また、上記実施の形態で説明した記憶手段14等はハードディスク600内に設けるのが好適である。

【0466】

このようなコンピュータ602の操作者は、上記各種プログラムを起動し、質問を生成し、団体のメンバーから得た回答をキーボード604から入力すること等を実行することができる。もちろん、回答の入力は、マウス等の入力デバイスを用いて実行してもかまわない。

【0467】

なお、図15においては、いわゆるスタンドアローンでプログラムがコンピュータ602上で動作する例を示したが、ネットワークを介してプログラムを供給する形態を採用してもよい。

【0468】

たとえばサーバに上記各種プログラムが格納されており、そのプログラムを実行する必要がある度に、クライアントコンピュータがサーバ内のプログラムを実行したり、ダウンロードして使用する形態を採用することも好ましい。

【 0 4 6 9 】

セキュリティポリシーのドラフトについて

これまで述べた各実施の形態 1 ～ 8 においては、セキュリティポリシーのドラフトの構築に関して主に述べたが、ドラフトではないセキュリティポリシーの構築に使用できることは言うまでもない。すなわちセキュリティポリシードラフト構築装置は、セキュリティポリシーの構築装置でもあり、セキュリティポリシーのドラフト構築の方法は、セキュリティポリシー構築方法でもある。また、ドラフト構築手段は、セキュリティポリシーの構築手段でもある。

【 0 4 7 0 】

【発明の効果】

以上述べたように、本発明によれば、団体のメンバーに質問をすることによって、その回答に基づき、セキュリティポリシーを構築している。したがって、セキュリティポリシーを容易に構築することができる。

【 0 4 7 1 】

さらに、本発明によれば、段階的にセキュリティポリシーの構築を行っているため、団体の要望（予算など）に応じた柔軟な構築方法を実行することが可能である。

【 0 4 7 2 】

また、本発明によれば、団体の情報セキュリティの状況を診断するので、団体は情報セキュリティの重要性を知ることができる。

【 0 4 7 3 】

また、本発明によれば、セキュリティ対策を優先度と共に知ることができるため、将来の情報セキュリティ対策の計画を立案しやすくなる。さらに、この計画に基づき、団体の予算の検討を行うことが可能となる。

【 0 4 7 4 】

また、本発明によれば、利用者が、セキュリティポリシーの構築に際して使用するグローバルガイドラインを指示可能である。

【 0 4 7 5 】

また、本発明によれば、グローバルガイドライン以外の特定の業種向けの規定

・ 勧告を使用してセキュリティポリシーを構築しているので、各業種により合致した緻密なセキュリティポリシーを構築可能である。

【 0 4 7 6 】

また、本発明によれば強度指標を用いて利用者がセキュリティポリシーの強度を指示可能である。また、本発明によれば、強度指標を用いてセキュリティポリシーの強度を調整することができる。

【 0 4 7 7 】

また、本発明によれば、利用者がセキュリティポリシーの構築範囲を明示的に指示可能である。その結果、団体の部分的なセキュリティポリシーの構築を実行することができる。

【図面の簡単な説明】

【図 1】

本発明の好適な実施の形態 1 のビジネスモデルの原理を表すフローチャートが示されている。

【図 2】

評価装置の構成ブロック図である。

【図 3】

評価書の作成作業の動作を表すフローチャートである。

【図 4】

セキュリティポリシードラフト構築装置の構成ブロック図である。

【図 5】

セキュリティポリシードラフト構築装置を用いてセキュリティポリシーのドラフトを構築する動作を表すフローチャートである。

【図 6】

職務内容を表すタイプの一覧表を示す図である。

【図 7】

分析装置の構成ブロック図である。

【図 8】

実施の形態 2 のセキュリティポリシードラフト構築装置の構成ブロック図であ

る。

【図 9】

実施の形態 3 のセキュリティポリシードラフト構築装置の構成ブロック図である。

【図 1 0】

実施の形態 4 のセキュリティポリシードラフト構築装置の構成ブロック図である。

【図 1 1】

実施の形態 5 のセキュリティポリシードラフト構築装置の構成ブロック図である。

【図 1 2】

実施の形態 5 のセキュリティポリシー強度調整装置の構成ブロック図である。

【図 1 3】

実施の形態 5 のセキュリティポリシー強度調整装置の動作を表すフローチャートである。

【図 1 4】

実施の形態 6 のセキュリティポリシードラフト構築装置の構成ブロック図である。

【図 1 5】

実施の形態 7 におけるコンピュータ及びその内部のハードディスクを示す説明図である。

【符号の説明】

- 1 0 評価装置
- 1 2 質問出力手段
- 1 4 記憶手段
- 1 6 回答保管手段
- 1 8 セキュリティ完成度作成手段
- 2 0 セキュリティポリシードラフト構築装置
- 2 2 質問生成手段

- 2 4 記憶手段
- 2 6 回答保管手段
- 2 8 ドラフト構築手段
- 3 0 分析装置
- 3 2 矛盾検査手段
- 3 4 仮想構築手段
- 3 6 実システム入力手段
- 3 8 差異出力手段
- 4 0 矛盾出力手段
- 4 1 整合手段
- 1 2 0 セキュリティポリシードラフト構築装置
- 1 2 2 質問生成手段
- 1 2 4 記憶手段
- 1 2 6 回答保管手段
- 2 2 0 セキュリティポリシードラフト構築装置
- 2 2 2 質問生成手段
- 2 2 4 記憶手段
- 2 2 6 回答保管手段
- 2 2 8 ドラフト構築手段
- 3 2 0 セキュリティポリシードラフト構築装置
- 3 2 2 質問生成手段
- 3 2 4 記憶手段
- 3 2 6 回答保管手段
- 3 2 8 ドラフト構築手段
- 4 2 0 セキュリティポリシードラフト構築装置
- 4 2 2 質問生成手段
- 4 2 4 記憶手段
- 4 2 6 回答保管手段
- 4 2 8 ドラフト構築手段

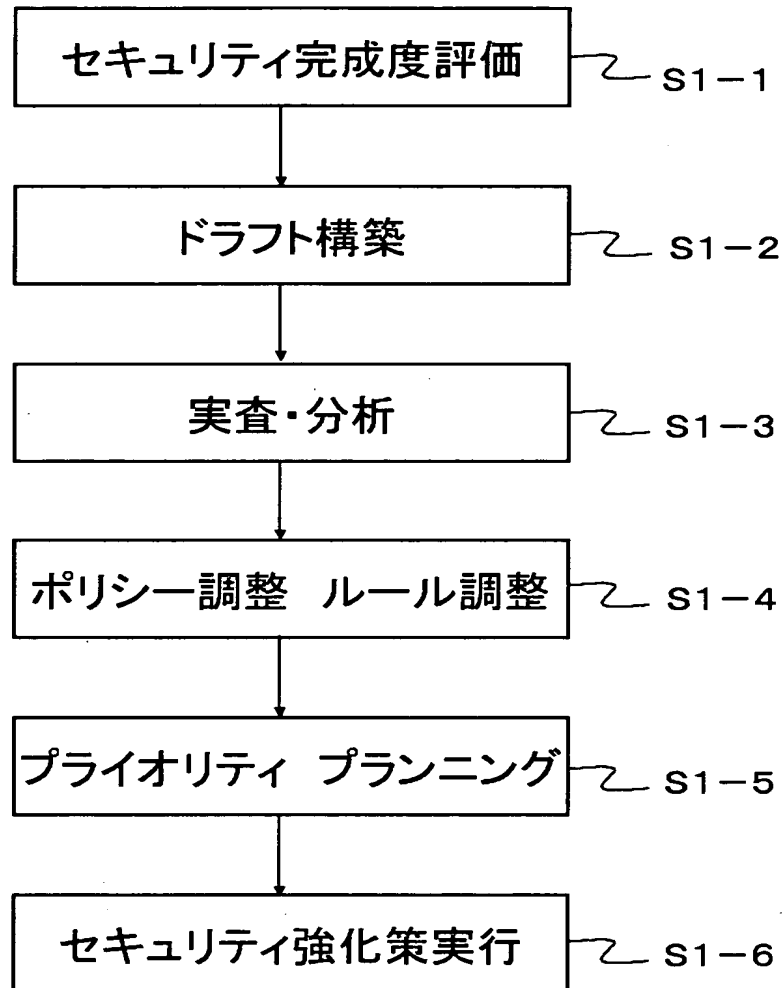
- 5 0 0 セキュリティポリシー強度調整装置
- 5 0 2 強度検査手段
- 5 0 4 強度調整手段
- 5 0 6 記憶手段
- 5 0 8 合成手段
- 5 2 0 セキュリティポリシードラフト構築装置
- 5 2 2 質問生成手段
- 5 2 4 記憶手段
- 5 2 6 回答保管手段
- 5 2 8 ドラフト構築手段
- 6 0 0 ハードディスク
- 6 0 2 コンピュータ
- 6 0 4 キーボード

【書類名】 図面

【図1】

図1

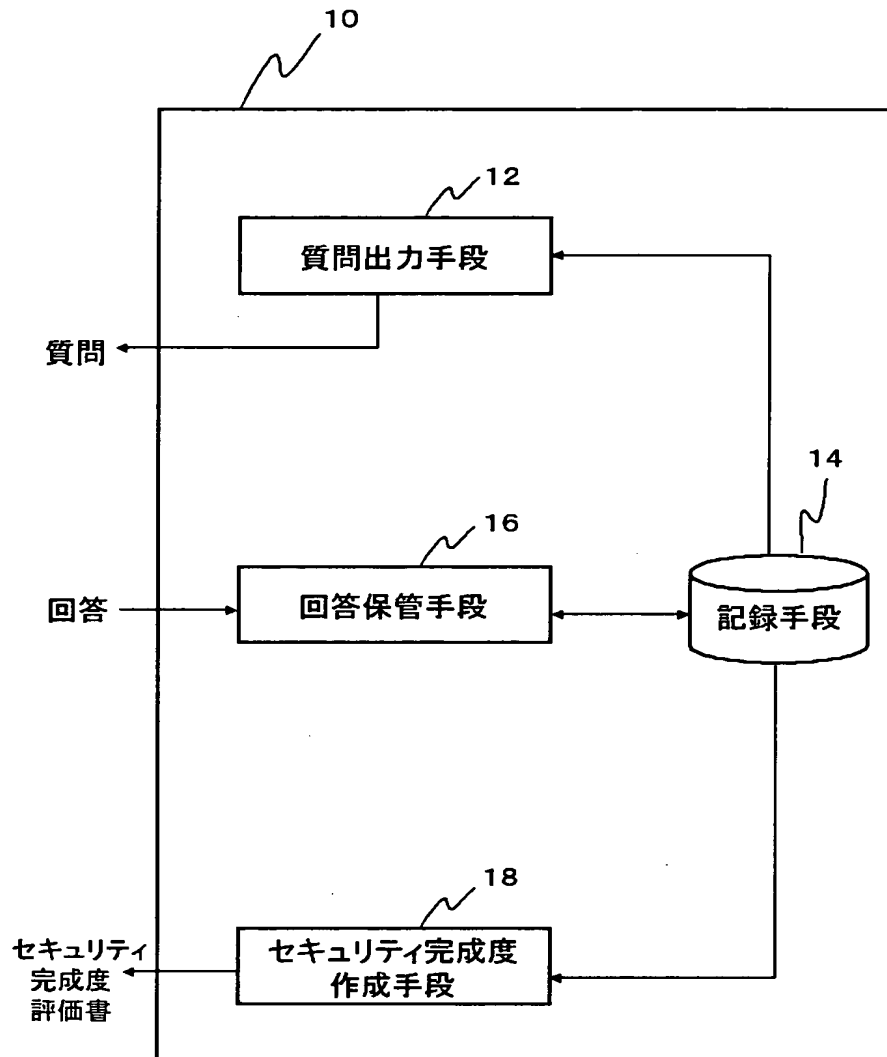
ASG-0002



【図 2】

図2

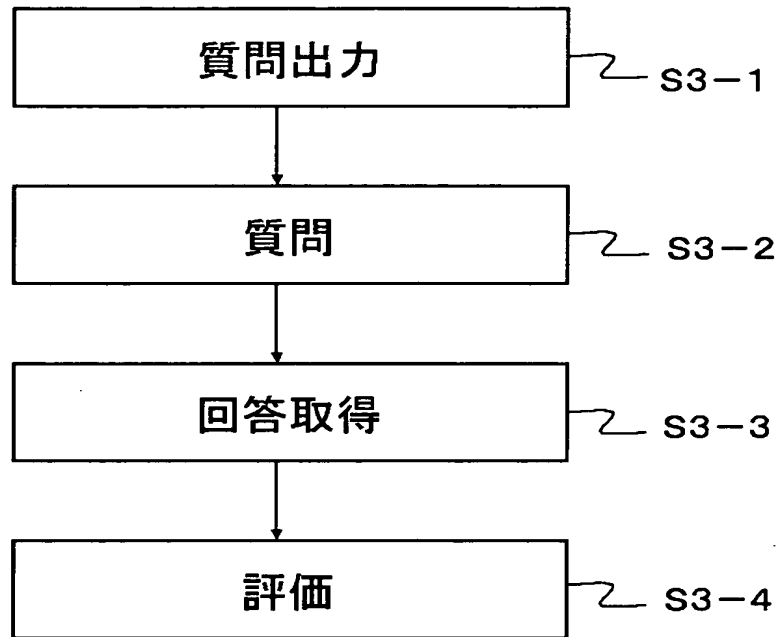
ASG-0002



【図 3】

図3

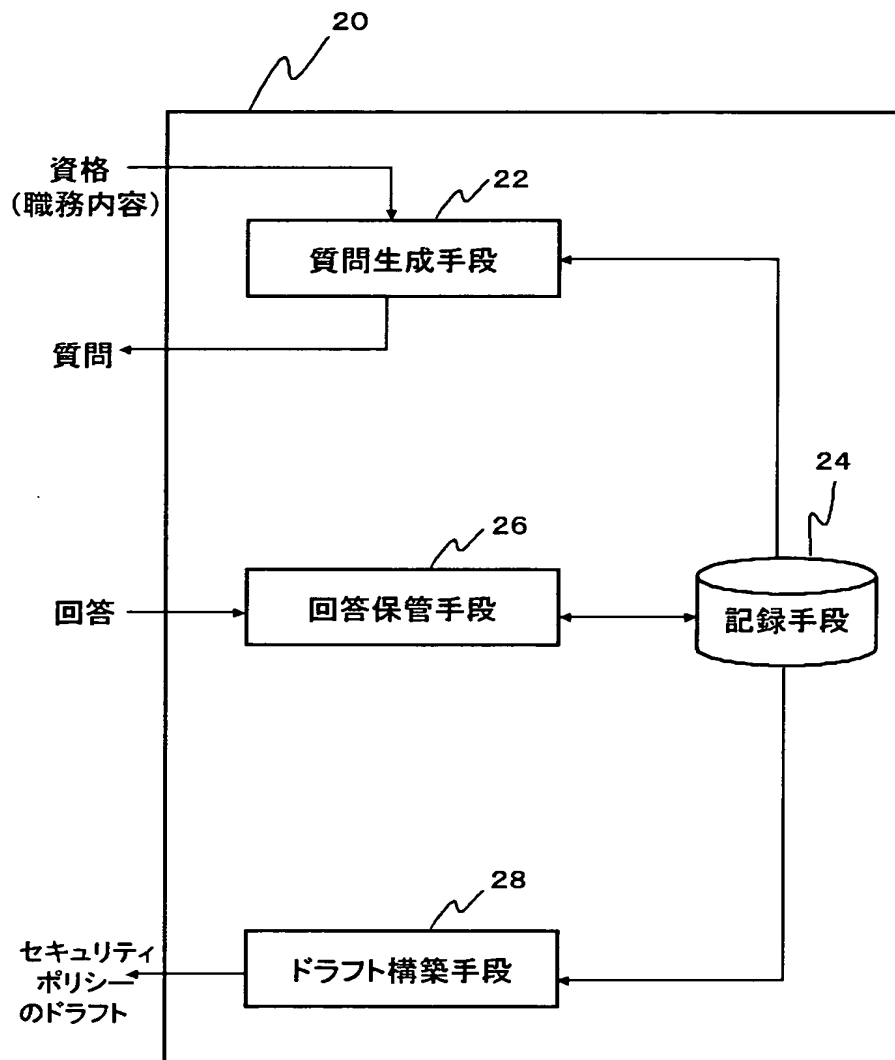
ASG-0002



【図 4】

図 4

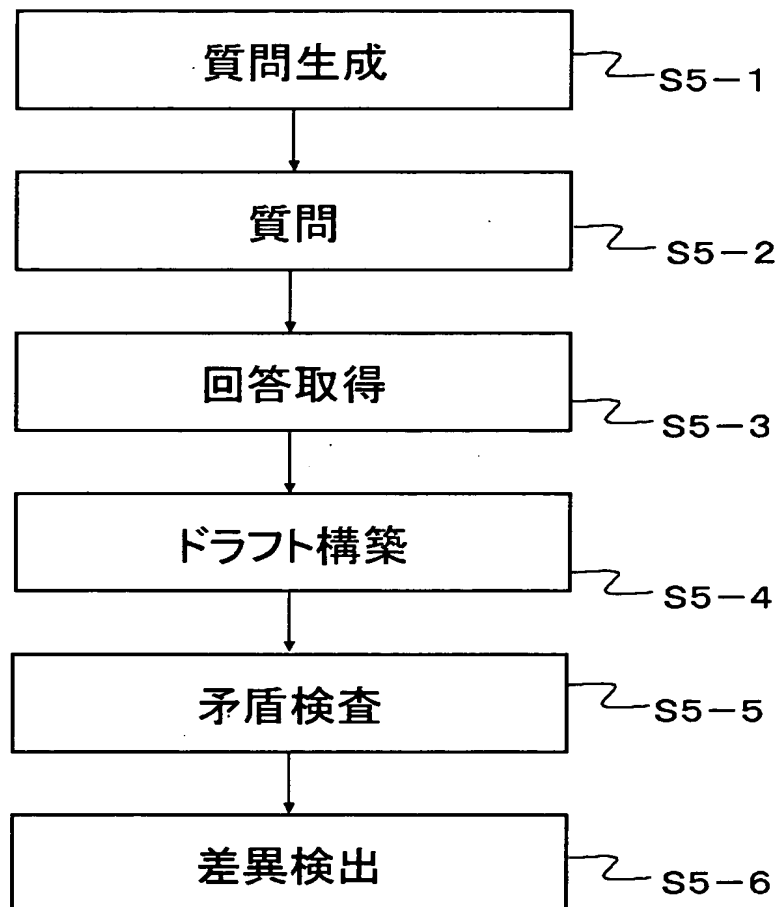
ASG-0002



【図 5】

図5

ASG-0002



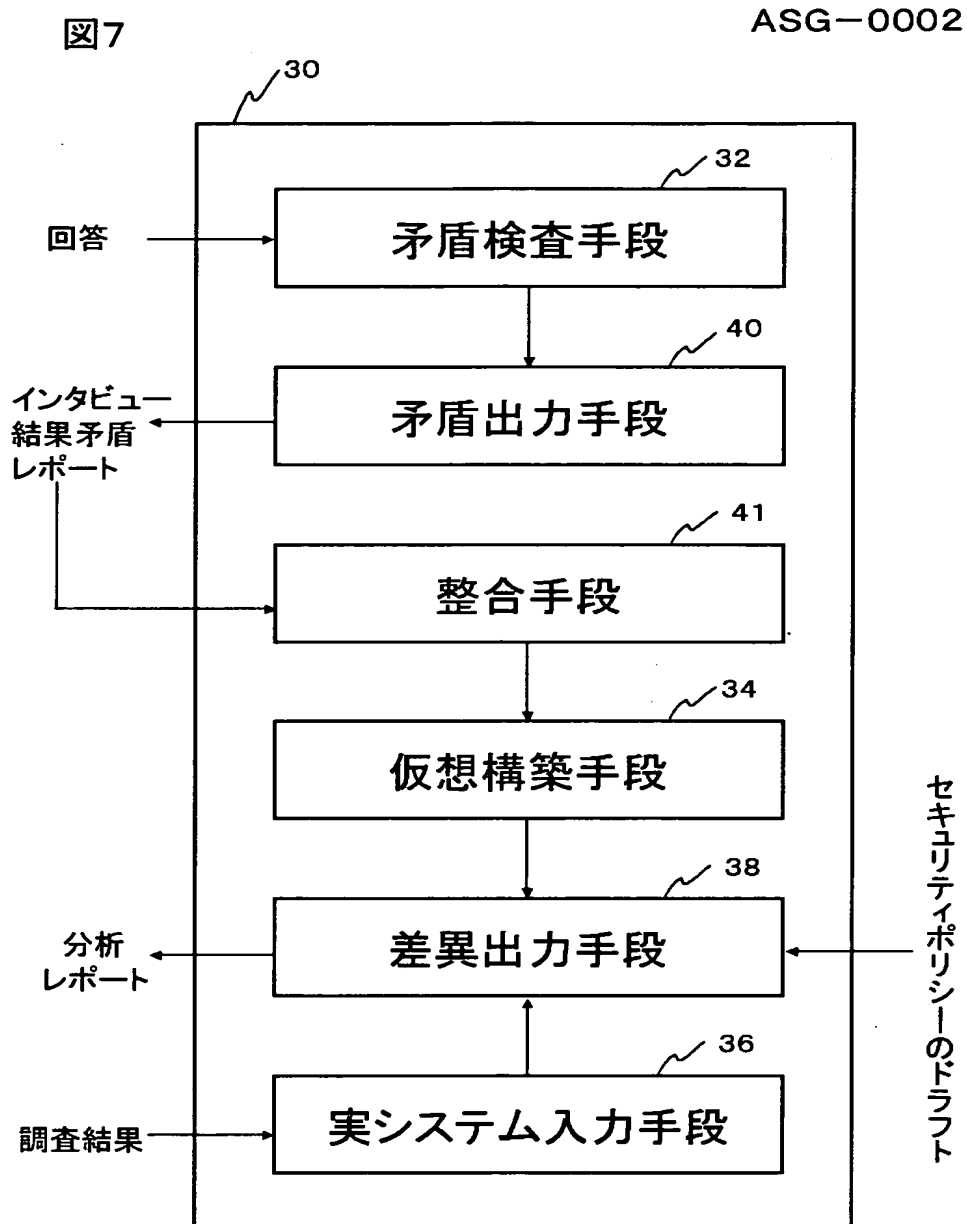
【図 6】

図 6

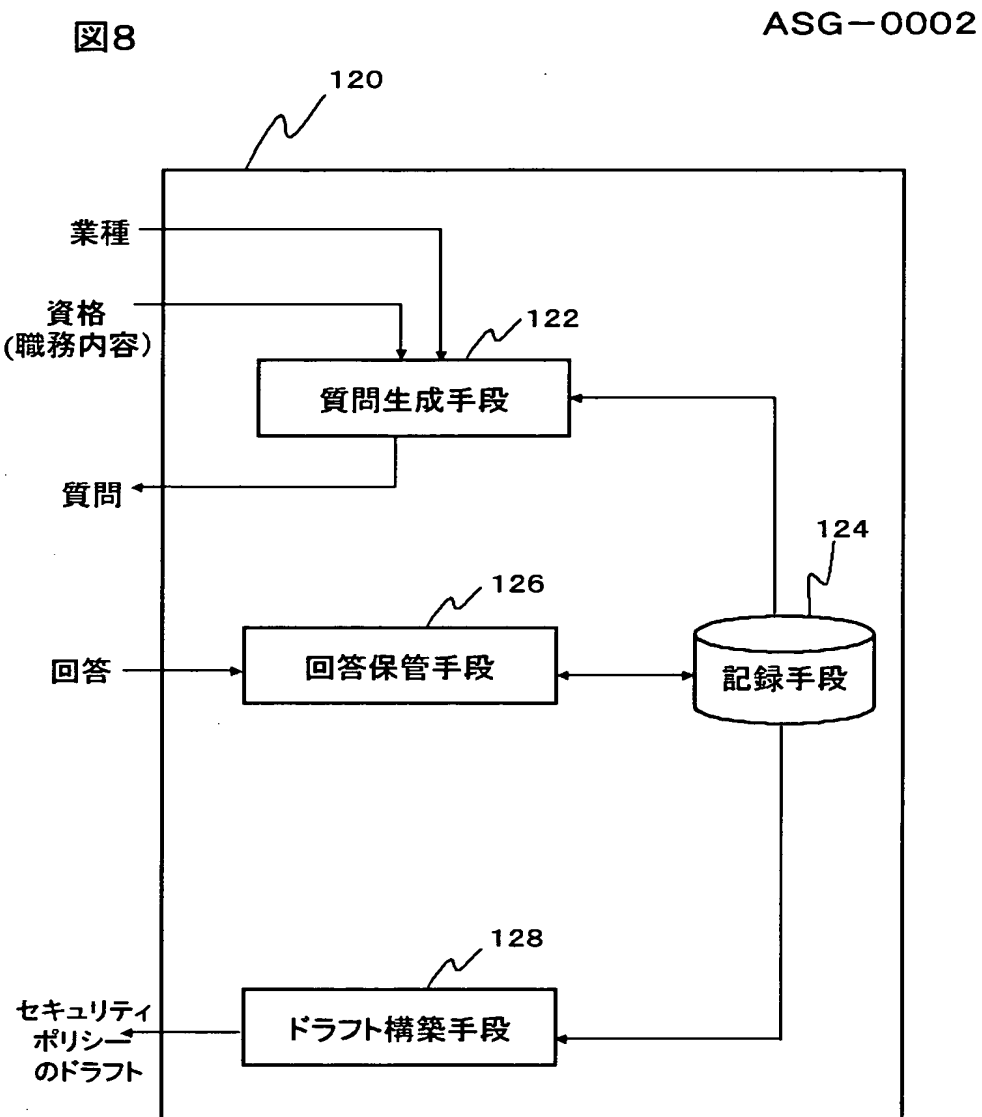
ASG-0002

タイプ	定義
アプリケーション管理者[APP]	アプリケーション、またはアプリケーションのグループの運用管理者
アプリケーションセキュリティ管理者[ASA]	アプリケーション、またはアプリケーションのグループのローカルセキュリティ運用管理者
内部監査役員[AUD]	内部監査を担当する役員
社長／最高経営責任者[CEO]	社内の業務、運営、またはその他全般に関わる最終決定権を持つ役員、または社長。
情報統括役員[CIO]	情報統括役員。単なるコンピュータ担当者とは違い、企業戦略として情報システムの活用方法を立案、実行する情報資源管理の責任をもつ。情報、通信部門の最高責任者でもある。
災害復旧統轄役員[DDR]	災害復旧を担当する上級役員
ダイヤルイン管理者[DIA]	ネットワークセグメント、または部門のダイヤルイン担当の管理者
情報保護役員[DIP]	情報セキュリティ担当の役員
災害復旧管理者[DRA]	ネットワークセグメント、ホストまたはアプリケーションについての各部のセキュリティ管理者
部門セキュリティ管理者[DSA]	ローカルのネットワークセグメント、ホスト、またはアプリケーションについての各部のセキュリティ管理者
通信担当役員[DTC]	電話回線、広範囲なネットワーク接続を含む電気通信を担当する役員
Facilitator[FAC]	インタビュー実施者
ファイアウォール管理者[FWA]	ファイアウォールのホストシステムの運用管理者
人事[HR]	従業員の採用、教育を担当する部門
ホスト管理者[HST]	ローカルホスト、またはローカルホストのグループ運用管理者
法律担当役員[LEG]	法律顧問
ネットワークセグメント[Net]	ネットワークセグメント、またはネットワークセグメントのグループ運用管理者
ユーザデスクトップ管理者[PCA]	ローカルユーザデスクトップコンピュータを担当する運用管理者

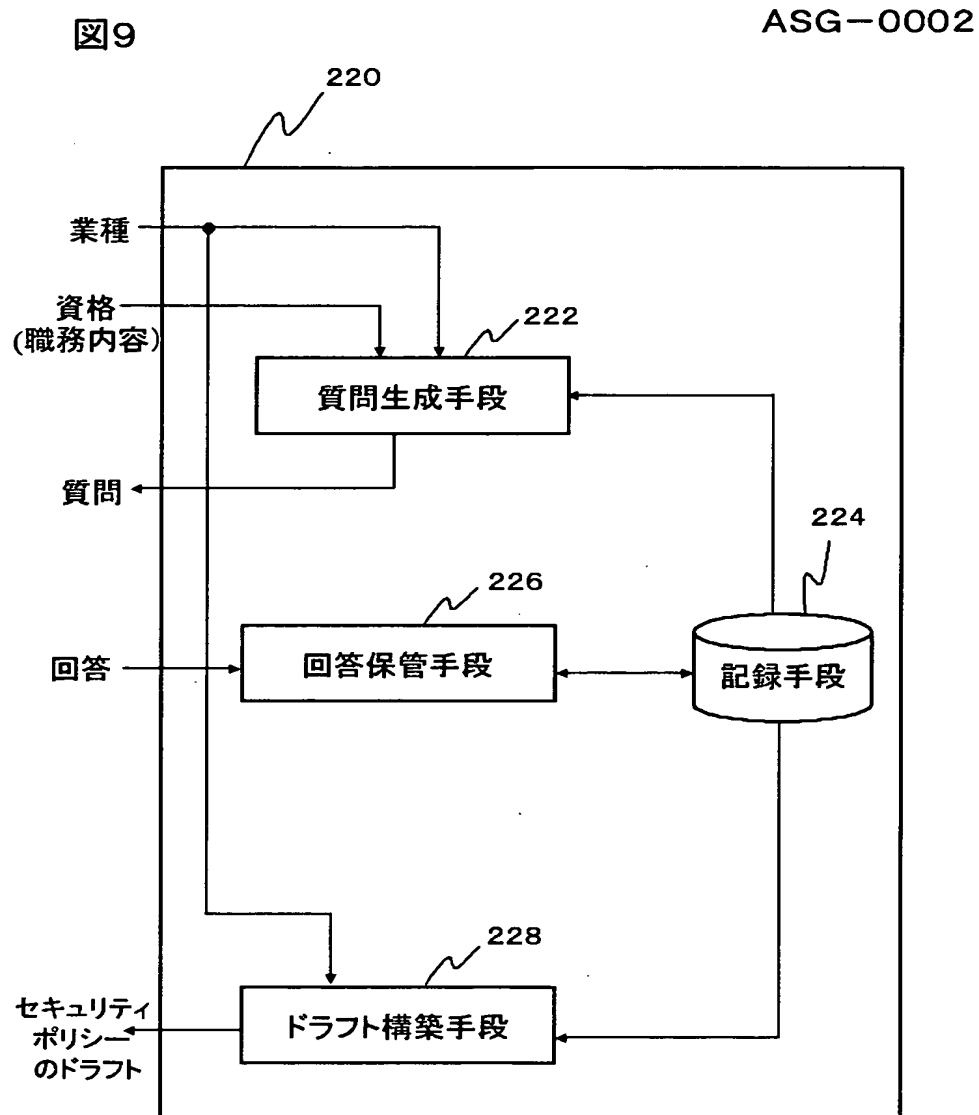
【図 7】



【図 8】



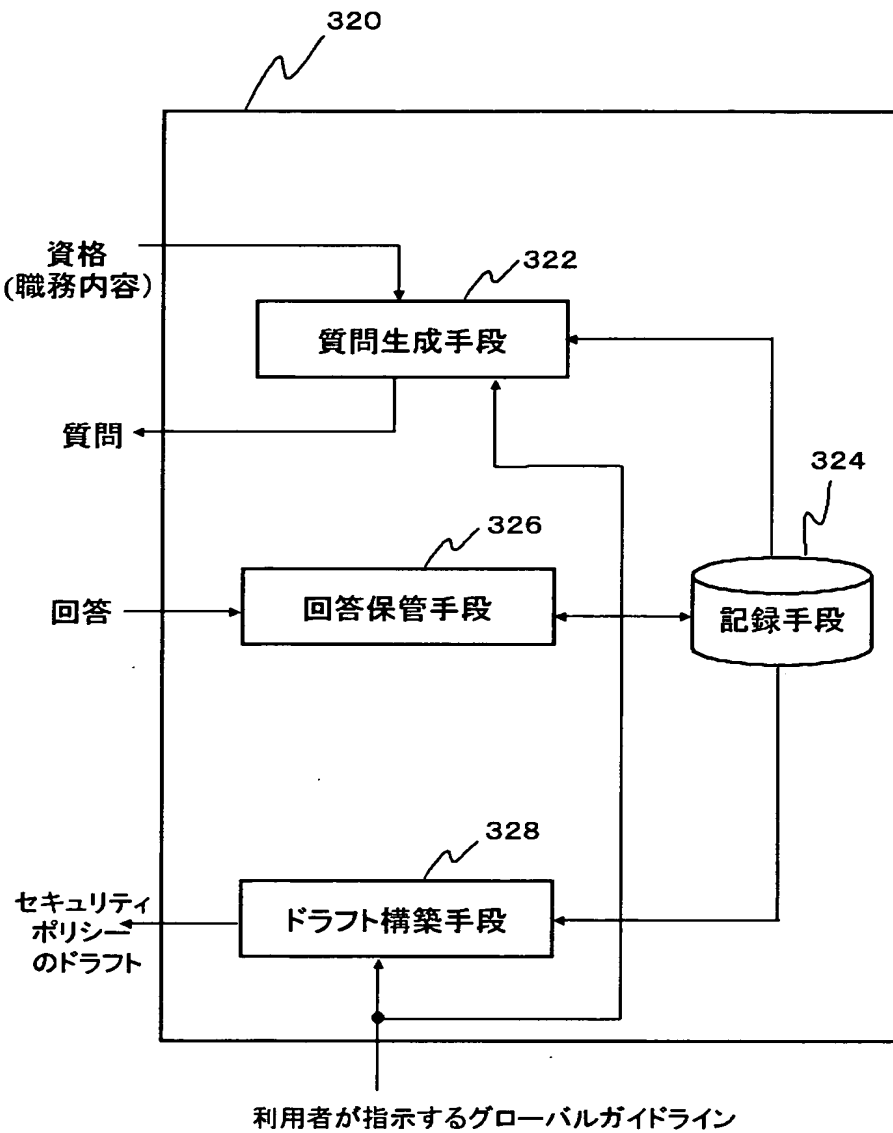
【図 9】



【図 1 0】

図10

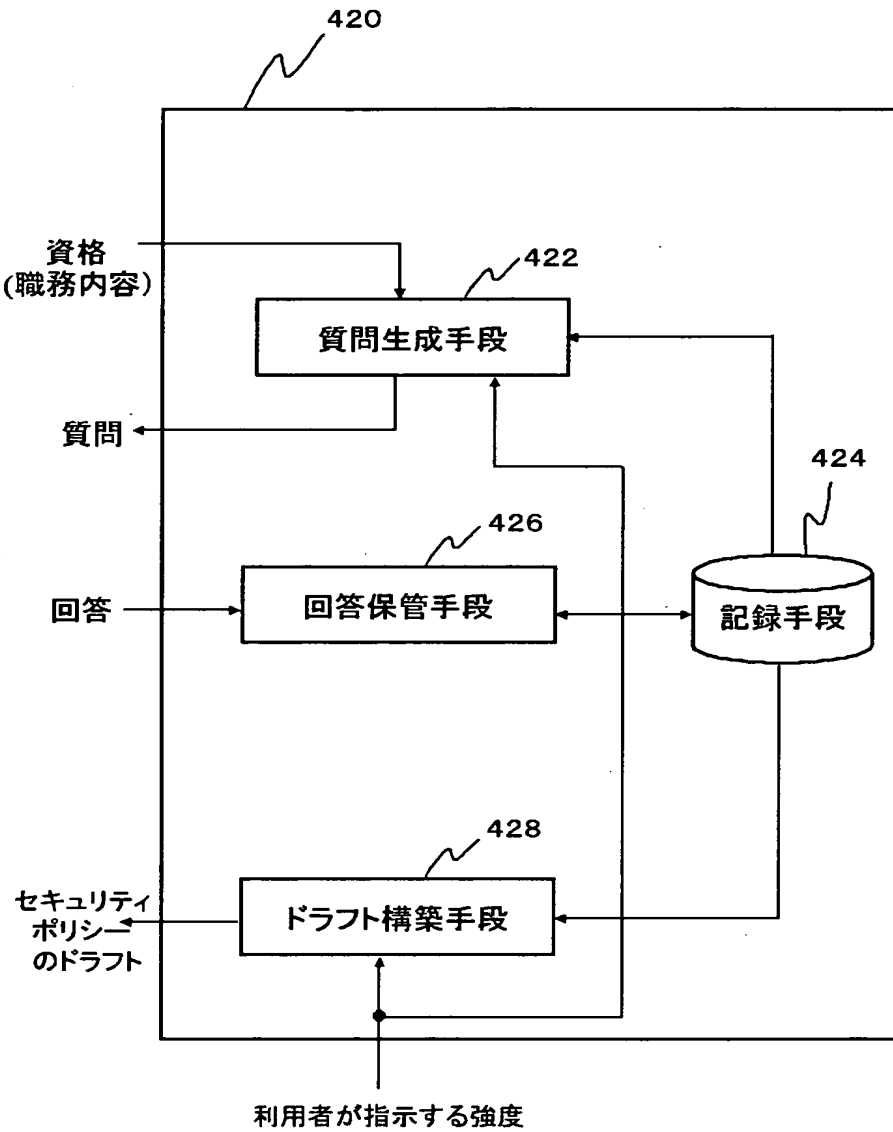
ASG-0002



【図 11】

図 11

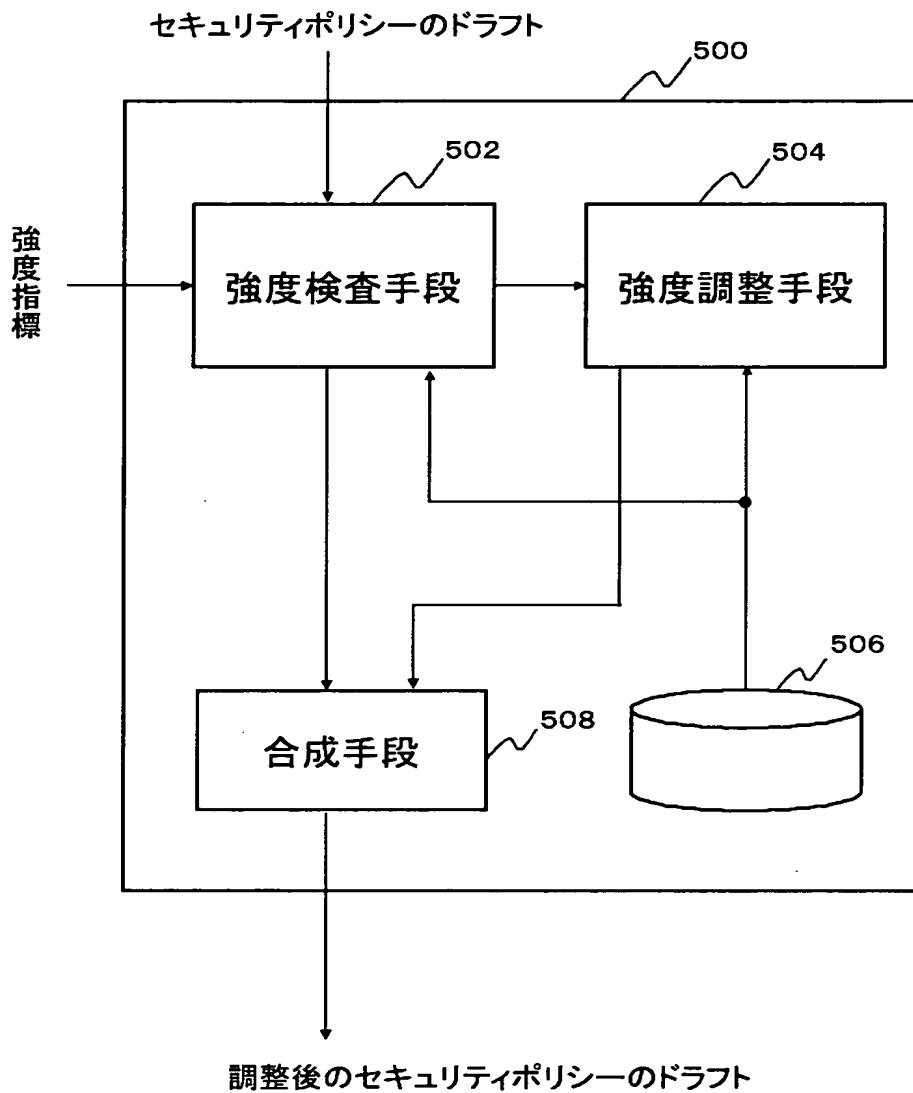
ASG-0002



【図12】

図12

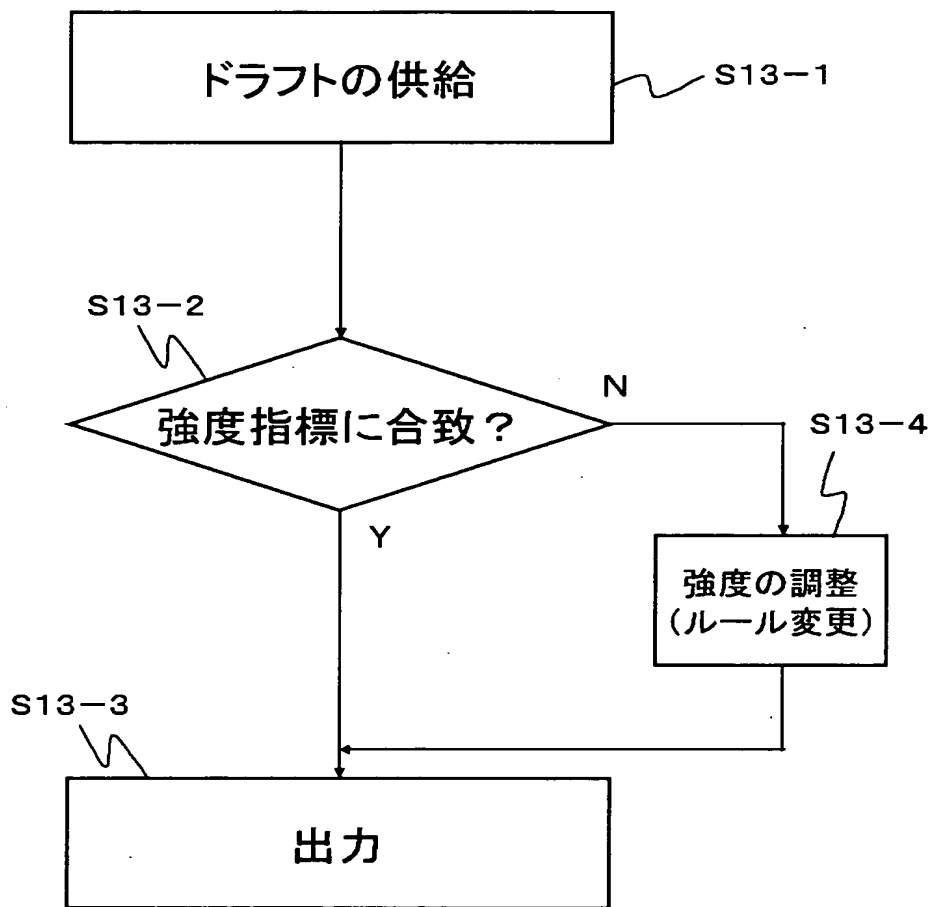
ASG-0002



【図13】

図13

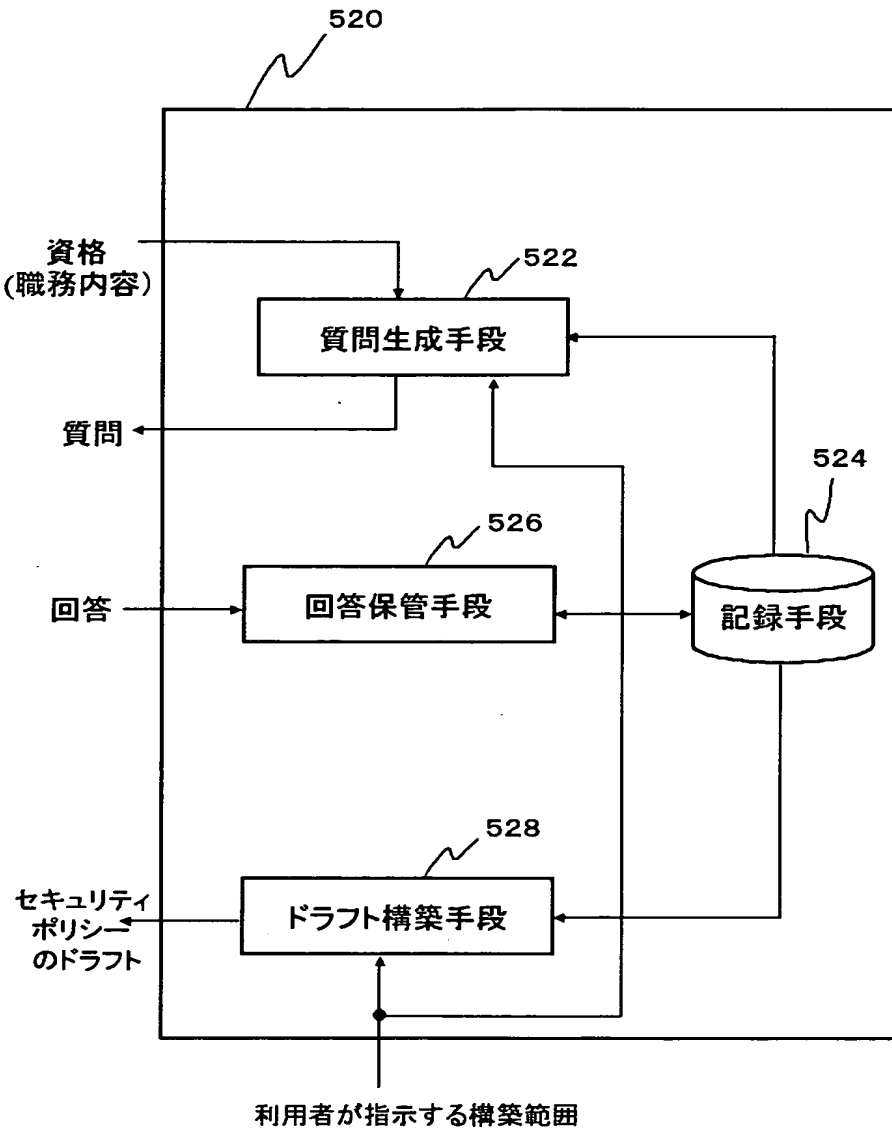
ASG-0002



【図14】

図14

ASG-0002

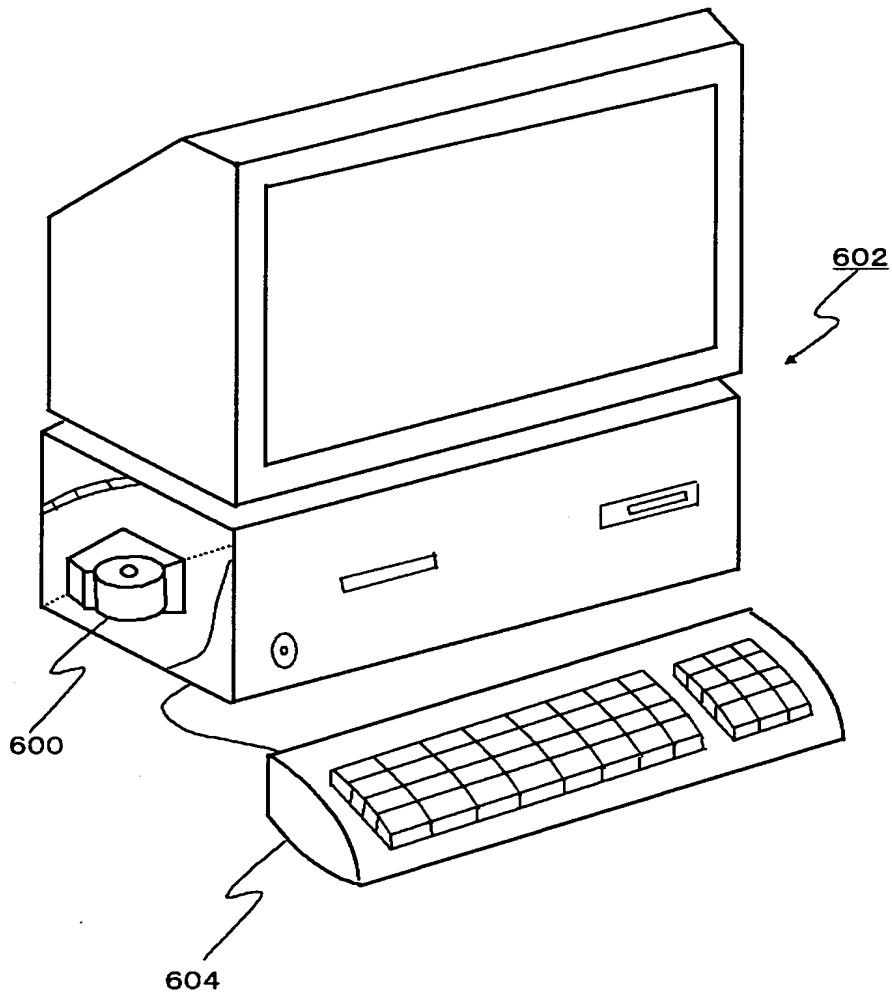




【図 15】

図 15

ASG-0002



【書類名】 要約書

【要約】

【課題】 セキュリティポリシーを効率的に構築する方法及びセキュリティポリシーの構築を支援する装置を提供することである。

【解決手段】 6段階のステップからなるセキュリティ構築手法によれば、最初
は簡易にセキュリティポリシーのドラフトを構築し、必要に応じ、団体の実態と
の再調整を行い、段階的に、セキュリティポリシーを完成していくので、各団体
のスケジュールや予算に合わせてセキュリティポリシーを構築することが可能で
ある。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [500056448]

1. 変更年月日	2000年 2月10日
[変更理由]	新規登録
住 所	東京都中央区日本橋小網町19-7
氏 名	株式会社アズジェント